CYBERGUARD COMPLIANCE

indio™

System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Indio Technologies, Inc.'s Indio System Based On the Trust Services Criteria for Security, Availability, and Confidentiality

For the Period November 1, 2021 to October 31, 2022

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Indio Technologies, Inc.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over Indio Technologies, Inc.'s Indio System Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion) that Indio Technologies, Inc.'s controls over the Indio System (System) were effective throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that its principal 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* (AICPA, *Trust Services Criteria*).

The Assertion also indicates that Indio Technologies, Inc.'s ("Service Organization" or "Indio") controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Indio's infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Indio uses a subservice organization to provide 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 to achieve Indio'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. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitable design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Indio management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Indio System and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Indio System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of Indio's System relevant security, availability, and confidentiality policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Indio's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve Indio's Indio System's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

In our opinion, management's assertion that the controls within Indio's Indio System were effective throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that Indio'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

November 16, 2022
Las Vegas, Nevada

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

Scope

We, as management of Indio, are responsible for:

- Identifying the Indio's Indio System (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled Indio Technologies, Inc.'s Description of the Indio System (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment B)
- Identifying, designing, implementing, operating, and monitoring effective controls over Indio's Indio System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period November 1, 2021 to October 31, 2022.

Indio uses a subservice organization to provide 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, to achieve Indio'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.

We assert that the controls within the system were effective throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice

organizations and user entities applied the complementary controls assumed in the design of Indio's Indio System controls throughout the period November 1, 2021 to October 31, 2022.

Indio Technologies, Inc.

ATTACHMENT A: INDIO TECHNOLOGIES, INC.'S DESCRIPTION OF ITS INDIO SYSTEM

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

The Indio Platform is hosted in Amazon Web Services (AWS) across multiple Availability Zones for redundancy and disaster recovery purposes. Indio Technologies, Inc. does 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 Indio Technologies, Inc. is responsible for securing the Indio Platform 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 Indio Technologies, Inc.'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 Indio Technologies, Inc.'s 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 Indio Technologies, Inc.'s 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 Indio System runs 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.

Indio Technologies, Inc. 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
- 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
- New Relic – Monitoring and alerting
- Figma – Vector graphics editor and prototyping tool

Data

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

Indio Technologies, Inc. stores and processes contact data within the Indio Technologies, Inc. System platform. 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.

Under a managed services agreement, Indio Technologies, Inc. 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. 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 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 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 Technologies, Inc. is 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. Indio Technologies, Inc. endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

Indio Technologies, Inc. leverages 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 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 the Indio Platform. All IT 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.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect Indio Technologies, Inc.'s service commitments or 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's controls are suitably designed and operating effectively at the subservice organizations, along with related controls at Indio.

Description of Complementary User Entity Controls

Indio controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of Indio's controls are suitably designed and operating effectively, along with related controls at Indio.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Company Background

Indio Technologies, Inc. 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 a high availability, 24/7 access for customers.

Description of Services Provided

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

The Indio Platform 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.

Principal Service Commitments and System Requirements

Indio Technologies, Inc.'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 the customer-facing website.

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

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

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the Indio platform and the customer data in accordance with Indio Technologies, Inc.'s security requirements.
- Perform annual third-party security 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 (currently using Trust Foundry)
- Use 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 formal access management procedures for the request, approval, provisioning, review, and revocation of Indio Technologies, Inc. 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 Technologies, Inc. establishes 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 Indio's 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 Technologies, Inc. regularly reviews the security, availability, and confidentiality commitments and performance metrics to ensure these commitments are met.