EXECUTIVE SUMMARY

Pursuant to Broward College Policy 6Hx2-1.14 and Procedure A6Hx2-1.14, Broward College exercised the authority delegated by the Board to issue a standard agreement (purchase order) with 7taps OpCo LLC for the license use of their Microlearning platform to design high-quality micro training options using AI-based interactive training for Broward College students, businesses, and the community. To market and increase student enrollment, capture leads, drive website traffic, and increase revenue. Fiscal Impact: $1,500.00

Presenter(s): Steven Tinsley, Vice President, Workforce Education and Strategic Partnerships

What is the purpose of this contract and why is it needed? The purpose of this agreement is to design and provide microlearning programs using research-based AI technology with a user-friendly interface to develop in-demand, innovative short programs to increase student enrollment.

What procurement process or bid waiver was used and why? Small purchase for Category One ($0.00 - $10,000) per College Procedure A6Hx2-6.34 was used, where there are no formal or informal competitive requirements for goods and services acquired by the College at this dollar threshold. Membership dues, per Florida Statute 119.01(3) require that all financial, business, and membership records held by the organization with the individual(s) or organization(s) for whom a purchase order is being issued are to be considered public records and shall be subject to the provisions of Florida Statute 119.07.

Is this a budgeted expenditure from the budget established at the last June Board of Trustees meeting? Yes, this expenditure was budgeted.

What fund, cost center and line item(s) were used?

- Fund: FD107
- Cost Center: CC0073
- GLC (General Ledger Code): 64500 - Other Services

Has Broward College used this vendor before for these products or services? Yes, we have used 7taps on a trial basis for six months.

Was the product or service acceptable in the past? Yes, the product was acceptable.

Was there a return on investment anticipated when entering this contract? Yes, there was an anticipated return on investment using 7taps.

Was that return on investment not met, met, or exceeded, and how? Yes. Continuing Education launched six-microlearning programs, with enhanced curriculum, using 7taps.

Does this directly or indirectly feed one of the Social Enterprise tactics and how? This directly feeds into the Social Enterprise strategy:

1. **Empower Student Development**, as it provides the learner with a customized learning experience designed based on student and community (partners) needs.

2. Provide a Best-in-Class Student Experience, using aspirational enhancements to our services and programs while monitoring student sentiment and needs.

Did the vendor amend Broward College's legal terms and conditions [to be answered by the Legal Office] **if the College's standard contract was used and was this acceptable to the Legal Office?**

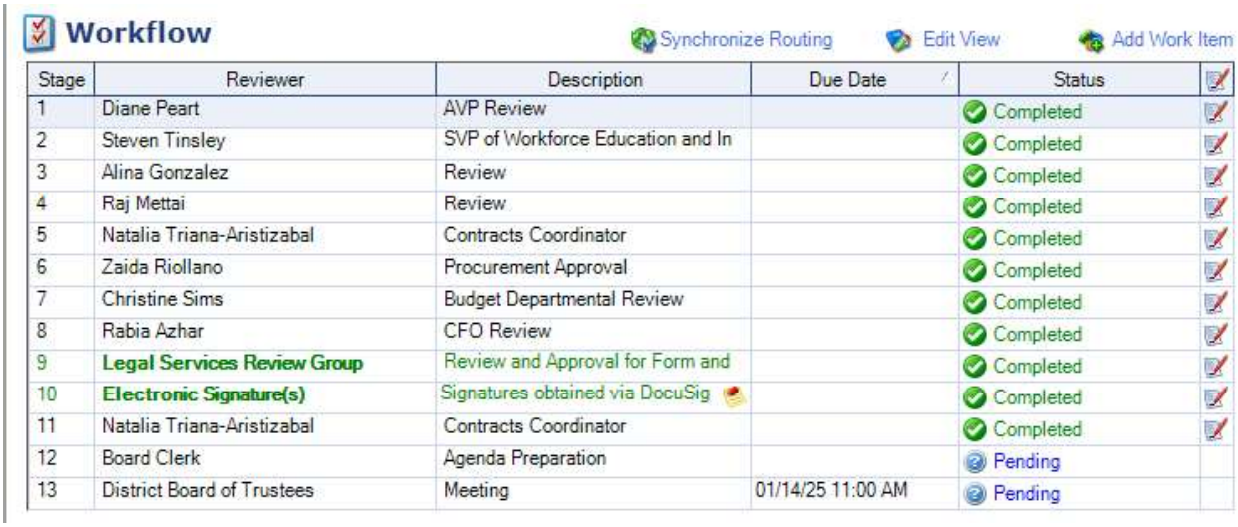
The General Counsel's office has reviewed the agreement and any deviation to the College's standard terms has been deemed acceptable.

FISCAL IMPACT:

Description: $1,500.00, this is an annual subscription for cost center CC0073, BU060. FD107, PG000513.

08/20/24	**CC0073 · Continuing Ed / Economic Development**	**($1,500.00)**

APPROVAL PATH: 12375 7taps OpCo LLC - Microlearning Platform



Workflow

Synchronize Routing | Edit View | Add Work Item

Stage	Reviewer	Description	Due Date	Status
1	Diane Peart	AVP Review		Completed
2	Steven Tinsley	SVP of Workforce Education and In		Completed
3	Alina Gonzalez	Review		Completed
4	Raj Mettai	Review		Completed
5	Natalia Triana-Aristizabal	Contracts Coordinator		Completed
6	Zaida Riollano	Procurement Approval		Completed
7	Christine Sims	Budget Departmental Review		Completed
8	Rabia Azhar	CFO Review		Completed
9	**Legal Services Review Group**	Review and Approval for Form and		Completed
10	**Electronic Signature(s)**	Signatures obtained via DocuSig		Completed
11	Natalia Triana-Aristizabal	Contracts Coordinator		Completed
12	Board Clerk	Agenda Preparation		Pending
13	District Board of Trustees	Meeting	01/14/25 11:00 AM	Pending

7taps | #1 Microlearning Platform

QUOTE

Quote Number: 2645

Issue Date: Wednesday, June 5, 2024 (Valid for 45 days after issue date)

From:

7taps Microlearning | support@7taps.com

Attention:

Diane Peart | dpeart@broward.edu

Name	Unit price	Quantity	Description	Amount
7taps Enterprise Edition One User License 1 Year [7TAPS-ENT1-L1-1YR]	$1,500.00	1	7taps Enterprise Edition Annual - 1 Year - 1 Creator	$1,500.00

Subtotal: $1,500.00

Total: $1,500.00

Amount Due: $1,500.00

Accepted by:	Donald Astrab
Signature:	Signed by: Donald Astrab
Start Date:	11/18/2024

This Purchase Order, along with the Broward College Purchase Order/Supplier Contract for Commodities and Service Terms and Conditions and the Broward College Supplemental Addendum - Software, constitute a binding contract between the College and the Vendor named on the Purchase Order when accepted by the Vendor either by express acknowledgment or by commencement of work or shipment without reservations.

7taps OpCo, LLC.
134 NE 1st Avenue, Delray Beach FL 33444

Product Pricing

BROWARD COLLEGE

BROWARD COLLEGE
SUPPLEMENTAL ADDENDUM - SOFTWARE

1. Incorporation by Reference. The District Board of Trustees of Broward College, Florida ("BC") and the undersigned ("Vendor") hereby incorporate this Supplemental Addendum–Software ("Addendum") into the agreement between BC and Vendor ("Agreement"). If this Addendum conflicts with the Agreement terms, this Addendum shall control.

2. Payment. Vendor shall submit bills for compensation for goods, services, and/or expenses in detail sufficient for a pre- and post-audit. Invoices may be submitted via email, facsimile or U.S. mail. The time at which payment will be due from BC will be approximately thirty (30) days from receipt of an undisputed invoice, acceptance of deliverables, and upon satisfaction of the BC conditions that are detailed herein. In lieu of all provisions in the Agreement pertaining to pentalites for late payment, if BC does not issue payment within approximately thirty days of receipt of a proper invoice, BC shall pay Vendor an interest penalty from the date the invoice was due until it was paid at the rate established pursuant to Section 55.03(1), Florida Statutes, if the interest exceeds one dollar.

3. Taxes. BC is immune and/or exempt from the payment of taxes and shall not be responsible for the payment thereof. BC shall provide an appropriate exemption certificate.

4. Travel Expenses. If BC is reimbursing travel expenses, Section 112.061, Florida Statutes, applies to those reimbursements. In order to be reimbursed, travel expenses must be expressly stated in the Agreement or otherwise approved by an authorized BC official in writing in advance.

5. No Automatic Renewals or Extensions. Provisions resulting in the automatic renewal or extension of the term of the Agreement shall be of no force and effect and are hereby deleted. To renew or extend the term of the Agreement, the parties shall enter into an amendment.

6. Compliance with Laws. Vendor represents, warrants and covenants as of the date of the Agreement and throughout the term of the Agreement that the software complies with all applicable legal requirements, including, but not limited to, the Americans with Disaiblities Act and related regulations.

7. Vendor Intellectual Property Indemnification. Vendor shall indemnify, defend, and hold harmless BC and its officers, directors, board of trustees, agents, assigns, and employees from liabilities, damages, losses, and costs, including but not limited to reasonable attorneys' fees, for any claim or lawsuit brought alleging infringement of any intellectual property right arising out of the rights granted by Vendor to BC under the Agreement. This section shall not be subject to any limitations of liability provisions in the Agreement. This paragraph shall survive the expiration or early termination of the Agreement.

8. Announcements and Press Statements. No party shall, except with prior written consent of the other party on each occasion, make any press or media announcements concerning the Agreement or use the name, logos, or trademarks of any other party, or any version, abbreviation, or representation of them, in any advertising or other form of publicity or fundraising without the written permission of the party whose name, logo, or trademark is sought for use. In the case of BC, permission must be granted by its _____ or that position's designee, and in the case of the other party, permission must be granted by its _____ or that position's designee.

9. Relationship of the Parties. Each of the parties is an independent contractor and nothing in the Agreement shall designate any of the employees or agents of one party as employees or agents of the other.

10. Use of BC Information Not Allowed. Pursuant to the Agreement, Vendor may access, maintain, collect, record, organize, structure, store, retrieve, adapt, alter, use, process or otherwise handle information owned or held by BC and may create information from or with such existing information owned or held by BC (collectively, the "BC Data"). Vendor shall not have the right to use BC Data (whatever the medium) except to perform its obligations under the Agreement. Without limitation of the foregoing, Vendor shall not give any third party access to BC Data without BC's written permission except as expressly authorized in the Agreement or this Addendum.

11. BC Rights in Information. BC retains all rights to, title to, and interest in BC Data, and Vendor's use and possession thereof is soley on BC's behalf. BC

may access and copy any BC Data in Vendor's possession at any time, and Vendor shall faciliate such access and copying promptly after BC's request.

12. Termination for Convenience. BC may terminate the Agreement upon thirty (30) days' notice to Vendor, with no further obligation to Vendor other than to pay for any amounts owing prior to the effective date of termination. BC shall not be liable for any early termination charges and shall not be entitled to any refund of prepaid amounts.

13. Annual Appropriation Contingency. The State of Florida's performance and obligation to pay under this Agreement is contingent upon an annual appropriation by the Legislature. In the event funding is not approved for any subsequent fiscal year, this Agreement shall terminate upon expenditure of the current funding, notwithstanding other provisions to the contrary. BC shall notify Vendor in writing after the adoption of the final budget for each subsequent fiscal year if funding is not approved.

14. State of Florida Public Entity Contracting Prohibitions. Vendor represents, warrants and covenants that it is not currently and, throughout the term of this Agreement shall not be, ineligible for the award or continuation of this Agreement under Sections 287.133, 287.134 and 287.135, Florida Statutes. Vendor understands and accepts that this Agreement may be void, voidable or subject to immediate termination by BC if the representation, warranty and covenant set forth above is violated. BC, in the event of such termination, shall not incur any liability to Vendor for any work or materials furnished.

15. BC's Sovereign Immunity. Nothing in the Agreement shall act, or be construed, to increase or alter BC's liability for tort claims beyond the waiver of immunity limits set forth in Section 768.28, Florida Statutes

16. Governing Law and Other Legal Matters. The laws of the State of Florida shall govern all aspects of the Agreement without regard to any conflict-of-law principles. The exclusive venue of any legal actions arising out of the Agreement shall be Broward County, Florida. BC is entitled to the benefits of sovereign immunity, including but not limited to immunity from suit in federal court. Any provisions in the Agreement requiring arbitration and/or mediation of matters arising out of or relating to the Agreement or altering the time to bring lawsuits or to make claims under the Agreement shall be of no force and effect and are hereby deleted. Any provisions resulting in the Agreement's causing a default under another agreement or otherwise triggering rights and responsibilities under another agreement between the parties shall be of no force and effect and are hereby deleted.

17. Confidentiality Obligations. Vendor shall comply with any and all applicable state and federal laws and BC policies and procedures governing the use and/or safekeeping of BC Data, including but not limited to the Family Educational Rights and Privacy Act, laws governing personally identifiable information, the Florida the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Federal Trade Commission's Red Flags Rule, and amendments thereto (collectively, "Privacy Laws"). In the Agreement involves Vendor's access to education records, Vendor is hereby designated a school official and will comply with all legal requirements applicable thereto. If the Agreement involves Vendor's access to, any protected health information, as that term is or may be defined by state or federal law, BC and Vendor shall enter into a separate business-associate agreement that shall govern the use of the protected health information.

In the event Vendor is required by subpoena, law, or other judicial or administrative process to disclose BC Confidential Information, Vendor shall (i) provide BC with prompt notice thereof; (ii) consult with BC on taking steps to resist or narrow such disclosure; (iii) furnish only that portion of BC Confidential Information that is responsive to the request; (iv) comply with the requirements of all Privacy Laws; and (v) reasonably cooperate with BC in any attempt that BC may make to obtain an order or other reliable assurance that confidential treatment shall be accorded.

Upon termination of the Agreement or upon request by BC, Vendor shall promptly return all BC Confidential Information. This section shall not be subject to any limitations of liability provisions in the Agreement. Vendor agrees to include all such terms and conditions in this section in any subcontractor or agency contracts providing services on behalf of Vendor, provided this requirement is not intended to authorize any subcontracting or agency unless permitted hereby.

18. Vendor's Confidential Information / Public Records Law. BC is subject to the public records

laws of Florida, including records retention requirements, and any provisions in the Agreement pertaining to confidentiality obligations on the part of BC are hereby deleted and shall be of no force and effect. Vendor shall allow public access to all project documents and materials in accordance with the provisions of Chapter 119, Florida Statutes. Should Vendor assert any exemptions to the requirements of Chapter 119 and related statutes, the burden of establishing such exemption, by way of injunctive or other relief as provided by law, shall be upon Vendor and Vendor shall bear all costs and fees related to the same.

If Vendor meets the definition of "contractor" under Section 119.0701, Florida Statutes, in addition to other Agreement requirements provided by law, Vendor must comply with public records laws, and shall:

(a) Keep and maintain public records required by BC to perform the service.
(b) Upon request from the BC, provide the BC with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law.
(c) Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the Agreement term and following completion of the Agreement if Vendor does not transfer the records to the BC.
(d) Upon completion of the Agreement, transfer, at no cost, to the BC all public records in possession of Vendor or keep and maintain public records required by the BC to perform the service. If Vendor transfers all public records to the BC upon completion of the Agreement, Vendor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If Vendor keeps and maintains public records upon completion of the Agreement, Vendor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the BC, upon request from the BC's custodian of public records, in a format that is compatible with the information technology systems of the BC
(e) IF VENDOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO VENDOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT BC AT (954) 201-7639, LEGALSERVICES@BROWARD.EDU, OR 111 EAST LAS OLAS BOULEVARD, #523, FORT LAUDERDALE, FL 33301.

IN ADDITION, VENDOR ACKNOWLEDGES THAT BC CANNOT AND WILL NOT PROVIDE LEGAL ADVICE OR BUSINESS ADVICE TO VENDOR WITH RESPECT TO ITS OBLIGATIONS UNDER THIS SECTION. VENDOR FURTHER ACKNOWLEDGES THAT IT WILL NOT RELY ON BC OR ITS COUNSEL TO PROVIDE SUCH BUSINESS OR LEGAL ADVICE, AND THAT VENDOR IS HEREBY ADVISED TO SEEK BUSINESS/LEGAL ADVICE WITH REGARD TO PUBLIC RECORDS MATTERS ADDRESSED BY THIS AGREEMENT. VENDOR ACKNOWLEDGES THAT ITS FAILURE TO COMPLY WITH FLORIDA LAW AND THIS AGREEMENT WITH RESPECT TO PUBLIC RECORDS SHALL CONSITUTE A MATERIAL BREACH OF THIS AGREEMENT AND GROUNDS FOR TERMINATION.

19. Miscellaneous. Any terms and/or conditions in the Agreement on the following subject matters are hereby deleted in their entirety and shall be of no force and effect: (i) grants of exclusivity by BC to Vendor; (ii) restrictions on the hiring of Vendor's employees; and (iii) attorneys' or collection-fees provisions.

By signing below, Vendor's authorized representative agrees to incorporate this Addendum into the Agreement, and hereby executes this Addendum as of the date set forth below.

VENDOR: 7TAPS OPCO LLC

By: Ezra Charm

Name: Ezra Charm

Title: COO

Date: August 1, 2024

7taps

SYSTEM AND ORGANIZATION CONTROLS (SOC) 2 TYPE 2
REPORT ON MANAGEMENT'S DESCRIPTION OF ITS

Microlearning Platform

And the Suitability of Design of Controls Relevant to the Controls Placed in Operation and Test of Operating Effectiveness Relevant to Security, Availability, and Confidentiality

For the period February 1, 2024 to April 30, 2024

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Table of Contents

1. Independent Service Auditors' Report

To the Management of 7Taps OpCo LLC (7Taps)

Scope

We have examined 7Taps' accompanying description of its Microlearning Platform titled "Description of 7Taps' Microlearning Platform" throughout the period February 1, 2024 to April 30, 2024 (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), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2024 to April 30, 2024, to provide reasonable assurance that 7Taps' 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).

7Taps uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 7Taps, to achieve 7Taps' service commitments and system requirements based on the applicable trust services criteria. The description presents 7Taps' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 7Taps' controls. 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 7Taps, to achieve 7Taps' service commitments and system requirements based on the applicable trust services criteria. The description presents 7Taps' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 7Taps' 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

7Taps 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 7Taps' service commitments and system requirements were achieved. 7Taps has provided the accompanying assertion titled "Assertion of 7Taps Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated

therein. 7Taps 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 Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of 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 American Institute of Certified Public Accountants. 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.

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
- 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 those tests are listed in section 4.

Opinion

In our opinion, in all material respects,

a. the description presents 7Taps' Microlearning Platform that was designed and implemented throughout the period February 1, 2024 to April 30, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period February 1, 2024 to April 30, 2024, to provide reasonable assurance that 7Taps' 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 organization and user entities applied the complementary controls assumed in the design of 7Taps' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period February 1, 2024 to April 30, 2024, to provide reasonable assurance that 7Taps' 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 7Taps' controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section 4, is intended solely for the information and use of 7Taps, user entities of 7Taps' Microlearning

Platform during some or all of the period February 1, 2024 to April 30, 2024, business partners of 7Taps subject to risks arising from interactions with the Microlearning Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who 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
- 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.

Sensiba LLP

San Jose, California

May 24, 2024

7taps

2. Assertion of 7Taps Management

We have prepared the accompanying description of 7Taps OpCo LLC's (7Taps) Microlearning Platform titled "Description of 7Taps' Microlearning Platform" throughout the period February 1, 2024 to April 30, 2024, (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). The description is intended to provide report users with information about the Microlearning Platform that may be useful when assessing the risks arising from interactions with 7Taps' system, particularly information about system controls that 7Taps 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, 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).

7Taps uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 7Taps, to achieve 7Taps' service commitments and system requirements based on the applicable trust services criteria. The description presents 7Taps' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 7Taps' 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 7Taps, to achieve 7Taps' service commitments and system requirements based on the applicable trust services criteria. The description presents 7Taps' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 7Taps' controls.

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

a. the description presents 7Taps' Microlearning Platform that was designed and implemented throughout the period February 1, 2024 to April 30, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period February 1, 2024 to April 30, 2024, to provide reasonable assurance that 7Taps' 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 organization and user entities applied the complementary controls assumed in the design of 7Taps' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period February 1, 2024 to April 30, 2024, to provide reasonable assurance that 7Taps' 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 7Taps' controls operated effectively throughout that period.

Signed by 7Taps Management
May 24, 2024

3. Description of 7Taps' Microlearning Platform

Company Background

7Taps is a microlearning platform designed to deliver engaging, bite-sized training content to employees. Founded in 2019 with the vision of simplifying and enhancing the learning experience, 7Taps leverages modern technology to create interactive, mobile-friendly courses that can be completed in just a few minutes. This approach not only fits into the busy schedules of today's workforce but also increases retention and engagement. The platform features easy-to-use course authoring tools and sharing capabilities, making it convenient for Learning & Development professionals to design effective learning modules quickly.

Services Provided

7Taps is a software-as-a-service (SaaS) platform that helps Learning & Development professionals create bite-sized interactive courses, share them with employees, and measure impact. The 7Taps platform consists of the following modules, all of which are covered by this report:

- Course authoring module: Allows the creation of bite-sized courses on any topic.
- Sharing capabilities: Allows the delivery of training materials to employees.
- Reporting module: Provides insights into employee performance and measures impact.
- Course viewer module. Allows the learners to access course content.

Principal Service Commitments and System Requirements

7Taps designs its processes and procedures related to its platform to meet its objectives for 7Taps microlearning services. Those objectives are based on the service commitments that 7Taps makes to user entities, the laws and regulations that govern the provision of 7Taps services, and the financial, operational, and compliance requirements that 7Taps has established for the services. The 7Taps microlearning services are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which 7Taps operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- Security principles within the fundamental designs of the 7Taps platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

7Taps establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in 7Taps' 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 7Taps platform.

Components of the System

Infrastructure

Primary infrastructure used to provide 7Taps system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Various Services, including VPC, Elastic IP, Security Group, Load Balancer	Proxies for inbound and outbound connections.
AWS	EKS	Container runtime for web services, APIs, job workers. Includes auto-scaling and self-healing to replace failed containers.
AWS	S3, RDS	Data storage for customer data and files.

Software

Primary software used to provide 7Taps system includes the following:

Primary Infrastructure	
Software	Purpose
GuardDuty	Security application used for automated intrusion detection (IDS)
WAF	Protects against common web exploits and bots that can affect availability, compromise security, or consume excessive resources.
Loki	Monitoring application used to provide monitoring, alter, and notification services for 7Taps platform

People

- Corporate.
  - Executives.
  - Senior operations staff.
  - Customer service representatives take support cases directly from customers.
  - Company administrative support staff, such as legal, compliance, accounting, finance, and human resources.

- Engineering.
  - The help desk group provides technical assistance to the 7Taps employees and platform users.
  - The software development staff develops and maintains the custom software. This includes the 7Taps Platform, supporting utilities, and the external websites that interact with the 7Taps Platform. The staff includes software developers, database administration, and software quality assurance.
  - Site reliability engineering staff supports the 7Taps Platform indirectly by monitoring internal and external security threats and maintaining current antivirus software.
  - Site reliability engineering staff maintains 7Taps' IT infrastructure, which is used by the software.

Data

Data, as defined by 7Taps, constitutes the following:

- Customer data
- Customer media files (images, video, audio)
- Error logs

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the 7Taps policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any 7Taps team member.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow 7Taps employees physical access. At present, 7Taps does not maintain any office space and all work is conducted remotely.

Logical Access

7Taps uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, 7Taps implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to cloud resources using Google GSuite for Single Sign-On (SSO). Users are also required to separately sign on to any systems or applications that do not implement Google SSO using passwords that conform to 7Taps security policies.

Employees accessing cloud resources are required to enable token-based (OTP) multi-factor authentication as supported by each service provider. All cloud-based services are accessed through SSL-secured connections.

Two days prior to a new employee's start date, their manager creates a list of employee access to be granted. Access rules have been pre-defined based on the defined roles.

On an annual basis, access rules for each role are reviewed by 7Taps' management team. As part of this process, the CTO reviews access by privileged roles and requests modifications based on this review.

Computer Operations – Backups

Customer data is backed up by 7Taps' operations team. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

7Taps monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. 7Taps evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Computing resources CPU utilization
- Database CPU utilization
- Disk storage
- Network bandwidth

7Taps has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. 7Taps system owners review proposed operating system patches to determine whether the patches are applied. Customers and 7Taps systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. 7Taps staff validate that all patches have been installed and if applicable that reboots have been completed.

7taps

Change Control

7Taps maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Engineering leads approve changes prior to release to the production environment.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

7Taps has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. 7Taps engineering team review proposed operating system patches to determine whether the patches are applied. 7Taps engineering team is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. 7Taps staff validate that all patches.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by 7Taps. The third party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by automated third-party tools on a quarterly basis in accordance with 7Taps policy. The automated third-party tools use industry standard scanning technologies and a formal methodology specified by 7Taps. These technologies are customized

to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Static code analysis scans and docker images scans are performed with each code change during continuous integration.

Authorized employees may access the system through the Internet using leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Services performed by 7Taps. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls:

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

7taps

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of 7Taps control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of 7Taps' ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

7Taps' management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.
Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

7Taps' management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

7Taps' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

7Taps' assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

7Taps' success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. 7Tap's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

7Taps' risk assessment process identifies and manages risks that could potentially affect 7Taps' ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. 7Taps identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by 7Taps, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

7Taps has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. 7Taps attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of 7Taps system; as well as the nature of the components of the system result in risks that the criteria will not be met. 7Taps addresses these risks through the implementation of

suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, 7Taps' management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of 7Taps' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At 7Taps, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all-hands meetings are held quarterly to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the all-hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate 7Taps personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. 7Taps' management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

7Taps' management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in 7Taps' operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of 7Taps' personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of

any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to 7Taps' Microlearning Platform.

Subservice Organizations

7Taps OpCo LLC's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to 7Taps' services to be solely achieved by 7Taps' control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of 7Taps.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - 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.	

7taps

Security Category	
Criteria	*Controls expected to be in place*
CC6.2 - 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.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.3 - 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.	
CC6.5 - 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 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - 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.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - 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.	AWS is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

7Taps OpCo LLC management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, 7Taps OpCo LLC performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization;
- Reviewing attestation reports over services provided by vendors and subservice organization; and
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

7Taps' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to 7Taps' services to be solely achieved by 7Taps' control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of 7Taps'.

7taps

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to 7Taps.
2. User entities are responsible for notifying 7Taps of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of 7Taps services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize 7Taps services.
6. User entities are responsible for providing 7Taps with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying 7Taps of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

7taps

4. Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and 7Taps related controls are an integral part of management's system description and are included in this section. Sensiba LLP performed testing to determine if 7Taps' controls were suitably designed and operating effectively to achieve the specified criteria for Security, Availability, and Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria), throughout the period February 1, 2024 to April 30, 2024.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of 7Taps activities and operations and inspection of 7Taps documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all 7Taps controls, this test was not listed individually for every control in the tables below.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
The entity has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	CC1.1.1	Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Code of Conduct upon hire.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	CC1.1.2	Inspected a background check for a sample of new hires to determine that background checks were completed for all new hires as a condition of their employment.	No exceptions noted
The entity has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	CC1.1.3	Inspected the entity's Acceptable Use Policy to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Acceptable Use Policy upon hire.	No exceptions noted
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	CC1.2.1	Inspected the information security policy to determine that management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC1.3.1	Inspected the organization chart review to determine that management reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	CC1.3.2	Inspected the information security policy to determine that management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
All entity's positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the entity.	CC1.4.1	Inspected a job description to determine that job requirements and responsibilities were documented.	No exceptions noted
New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	CC1.4.2	Inspected a background check for a sample of new hires to determine that background checks were completed for all new hires as a condition of their employment.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
The entity has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the entity's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	CC1.5.1	Inspected security awareness training confirmation for a sample of employees to determine that security awareness training was provided.	No exceptions noted
The entity Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC1.5.2	Inspected the security policies and acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
The entity conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	CC2.1.1	Inspected the Drata tool configurations to determine that the company uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	No exceptions noted
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
The entity has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	CC2.2.1	Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Code of Conduct upon hire.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
The entity Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC2.2.2	Inspected the security policies and acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
The entity maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	CC2.3.1	Inspected the entity's website to determine that the entity's privacy policies were posted.	No exceptions noted
The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	CC2.3.2	Inspected the company's Terms of Service to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC3.1.1	Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
CC3.2 - 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.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.2.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC3.2.2	Inspected the remediation plan to determine that Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.3.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC3.4.1	Inspected the organization chart review to determine that management reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.4.2	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
CC4.0 - Monitoring Activities			
CC4.1 - 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.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC4.1.1	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC4.1 - 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.			
The company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC4.1.2	Inspected the penetration test results to determine that the company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	No exceptions noted
CC4.2 - 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.			
The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC4.2.1	Inspected the entity's incident response policies and procedures to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted
The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	CC4.2.2	Inspected the support page to determine that the company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC5.0 - Control Activities			
CC5.1 - 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.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC5.1.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC5.1.2	Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC5.2.1	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted
The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC5.2.2	Inspected the remediation plan to determine that Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC5.3.1	Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted
The entity Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC5.3.2	Inspected the security policies and acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
CC6.0 - Logical and Physical Access Controls			
CC6.1 - 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.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	CC6.1.1	Inspected user accounts to determine that access to corporate network, production machines, network devices, and support tools requires a unique ID.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.1 - 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.			
The company requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	CC6.1.2	Inspected system configurations to determine that MFA was required in order to access sensitive systems and applications.	No exceptions noted
CC6.2 - 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.			
Prior to granting new hires access to system resources, HR must submit a completed access request form.	CC6.2.1	Inspected the access request form for a sample of new hires to determine that HR must submit a completed access request form prior to granting new hires access to system resources.	No exceptions noted
A termination checklist is completed to ensure that system access, including physical access, for terminated employees has been removed within one business day.	CC6.2.2	Inspected the termination checklist for a sample of terminated employees to determine that employee access to infrastructure is removed within one business day.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.3 - 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.			
The company's access reviews are performed on an annual basis.	CC6.3.1	Inspected the access review to determine that an access review was completed for the company on an annual basis.	No exceptions noted
CC6.4 - 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.			
The company relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's SOC 2 efforts.	CC6.4.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
CC6.5 - 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.			
The company has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	CC6.5.1	Inspected the Data Deletion Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
The company uses firewalls that ensure only approved connections, ports, and protocols are implemented.	CC6.6.1	Inspected firewall rules to determine that inbound and outbound traffic is appropriately restricted and allowed by exception.	No exceptions noted
The company requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	CC6.6.2	Inspected system configurations to determine that MFA was required in order to access sensitive systems and applications.	No exceptions noted
CC6.7 - 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.			
The company uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	CC6.7.1	Inspected TLS configurations to determine that the company uses appropriate encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	No exceptions noted
Customer data at rest is encrypted.	CC6.7.2	Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.7 - 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.			
The company ensures that company-issued laptops have encrypted hard-disks.	CC6.7.3	Inspected workstation and laptop encryption settings for a sample of computers to determine that full-disk encryption was implemented for all workstations and laptops.	No exceptions noted
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
The company requires antivirus software to be installed on workstations to protect the network against malware.	CC6.8.1	Inspected antivirus configurations for a sample of computers to determine that antivirus software was installed on workstations to protect the network against malware.	No exceptions noted
The company uses firewalls that ensure only approved connections, ports, and protocols are implemented.	CC6.8.2	Inspected firewall rules to determine that inbound and outbound traffic is appropriately restricted and allowed by exception.	No exceptions noted
CC7.0 - System Operations			
CC7.1 - 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.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC7.1.1	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.1 - 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.			
The company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC7.1.2	Inspected the penetration test results to determine that the company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	No exceptions noted
CC7.2 - 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.			
The company uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	CC7.2.1	Inspected the infrastructure logging configurations and alerts to determine that logging is implemented and alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	No exceptions noted
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC7.2.2	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.3 - 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.			
The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	CC7.3.1	Inspected the incident response policy to determine that policies and procedures related to resolving and escalating reported security issues were in place.	No exceptions noted
The company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	CC7.3.2	Inspected the incident tickets for a sample of security and privacy incidents to determine that the company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	N/A - A security or privacy incident did not occur during (February 1, 2024 – April 30, 2024) so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed the Incident Response Policy and security incident tracking tool to confirm the control was appropriately designed.
The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC7.3.3	Inspected the entity's incident response policies and procedures to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	CC7.4.1	Inspected the incident response policy to determine that policies and procedures related to resolving and escalating reported security issues were in place.	No exceptions noted
The company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	CC7.4.2	Inspected the incident tickets for a sample of security and privacy incidents to determine that the company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	N/A - A security or privacy incident did not occur during (February 1, 2024 – April 30, 2024) so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed the Incident Response Policy and security incident tracking tool to confirm the control was appropriately designed.
The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC7.4.3	Inspected the entity's incident response policies and procedures to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
The company has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	CC7.5.1	Inspected disaster recovery plan to determine that business and system recovery plans were documented and included roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted
The company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	CC7.5.2	Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
The company has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	CC8.1.1	Inspected the software development life cycle policy to determine that a software development life cycle policy was defined to ensure that appropriate controls were in place over the acquisition, development, and maintenance of technology and its infrastructure.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	CC8.1.2	Inspected the version control software to determine that version control software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	No exceptions noted
The company ensures that code changes are tested prior to implementation to ensure quality and security.	CC8.1.3	Inspected test results for a sample of changes to determine that code changes were tested prior to implementation.	No exceptions noted
The company's releases are approved by appropriate personnel prior to the release being implemented in production.	CC8.1.4	Inspected change tickets for a sample of changes to determine that releases were approved by appropriate personnel prior to the release being implemented in production.	No exceptions noted
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC9.1.1	Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC9.1.2	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
The company has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	CC9.1.3	Inspected the company's Business Continuity Plan to determine that it defined proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	CC9.2.1	Inspected the annual vendor review to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	No exceptions noted
The company has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	CC9.2.2	Inspected the vendor management policy to determine that a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships is defined.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
A1.0 - Additional Criteria for Availability			
A1.1 - 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.			
The company has implemented tools to monitor servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	A1.1.1	Inspected infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted
A1.2 - 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.			
The company relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's SOC 2 efforts.	A1.2.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
The company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	A1.3.1	Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
The company conducts annual BCP/DR tests and documents according to the BCDR Plan.	A1.3.2	Inspected the annual disaster recovery exercise to determine that the Company's disaster recovery plan is tested annually to ensure that recovery procedures are complete and accurate.	No exceptions noted
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
The entity establishes written policies related to retention periods for the confidential information it maintains.	C1.1.1	Inspected the data retention policy to determine that the entity established written policies related to retention periods for the confidential information it maintains.	No exceptions noted
The entity has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.	C1.1.2	Inspected the data classification policy to determine that the entity had established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that were required.	No exceptions noted
Customer data at rest is encrypted.	C1.1.3	Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted

7taps

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	C1.1.4	Inspected user accounts to determine that access to corporate network, production machines, network devices, and support tools requires a unique ID.	No exceptions noted
The company ensures that company-issued laptops have encrypted hard-disks.	C1.1.5	Inspected workstation and laptop encryption settings for a sample of computers to determine that full-disk encryption was implemented for all workstations and laptops.	No exceptions noted
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
Formal policies and procedures are in place to guide personnel in the disposal of any sensitive data.	C1.2.1	Inspected the Data Deletion Policy to determine that formal policies and procedures were in place to guide personnel in the disposal of any sensitive data.	No exceptions noted