BOULAY

Hit Labs, Inc. d/b/a Pronto

SOC 2 Type 1 Report

For the

Pronto Communication Platform

An Independent Service Auditor's Report on the
Suitability of the Design of Controls Relevant to Security

May 31, 2022

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Hit Labs, Inc. d/b/a Pronto:

Scope

We have examined Hit Labs Inc. d/b/a Pronto's ('Pronto' or the 'service organization') accompanying description of its communication system found in Section III titled "Description of the Pronto Communication Platform" as of May 31, 2022 (description) based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design of controls stated in the description as of May 31, 2022 to provide reasonable assurance that Pronto's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Pronto uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pronto, to achieve Pronto's service commitments and system requirements based on the applicable trust services criteria. The description presents Pronto's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Pronto's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Pronto, to achieve Pronto's service commitments and system requirements based on the applicable trust services criteria. The description presents Pronto's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Pronto's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Pronto 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 Pronto's service commitments and system requirements were achieved. In Section II, Pronto has provided the accompanying assertion titled "Management's Assertion" (assertion) about the description and the suitability of design of controls stated therein. Pronto 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 Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design 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 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 a description of a service organization's system and the suitability of the design 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
- 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
- Evaluating the overall presentation of the description

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

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

Inherent Limitations

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 report users may consider important to meet their information needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents Pronto's communication system that was designed and implemented as of May 31, 2022 in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of May 31, 2022 to provide reasonable assurance that Pronto's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of Pronto's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Pronto; user entities of Pronto's communication system as of May 31, 2022; business partners of Pronto subject to risks arising from interactions with the communication system, 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 services 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.

Minneapolis, Minnesota
October 4, 2022

SECTION II

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Hit Labs Inc. d/b/a Pronto's communication system titled "Description of the Pronto Communication Platform" as of May 31, 2022 (description) based on the criteria for a description of a service organization's system in *DC 200*, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the communication system that may be useful when assessing the risks arising from interactions with Pronto's system, particularly information about system controls that Pronto 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 (applicable trust services criteria) set forth in *TSP 100*, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Pronto uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pronto, to achieve Pronto's service commitments and system requirements based on the applicable trust services criteria. The description presents Pronto's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Pronto's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Pronto, to achieve Pronto's service commitments and system requirements based on the applicable trust services criteria. The description presents Pronto's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Pronto's controls.

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

a. the description presents the communication system that was designed and implemented as of May 31, 2022 in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of May 31, 2022 to provide reasonable assurance that Pronto's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Pronto's controls as of that date.

Ben Dolman

Ben Dolman
Co-Founder & Chief Technology Officer
Hit Labs, Inc. d/b/a Pronto

SECTION III

DESCRIPTION OF THE PRONTO COMMUNICATION PLATFORM

DESCRIPTION OF THE PRONTO COMMUNICATION PLATFORM

Company Background

Hit Labs, Inc. ('Pronto' or 'the Company') is a technology company that provides a communication platform that instantly connects people so they can learn faster, work smarter, and communicate seamlessly. The Company was founded in 2015 and is based in Lehi, Utah. For more information, please visit https://pronto.io/.

Description of Services Provided

The Pronto communication platform provides the following features:

- Instant Chat: Instant chat keeps team members connected for easy, asynchronous communication throughout the day.
- Groups: Joint collaboration is a must. Organize your people in small or large groups to enhance communication and engagement.
- Meetings: Take your meetings virtual so that everyone can join from wherever they are.
- Real-Time Translation: Avoid language challenges with real-time translation. Allow people to communicate in their preferred language for better connection.
- Search: Keep track of important information within your communications and keep up with what you need quickly, easily, and effectively.
- File-Sharing: Share documents alongside your regular communication feature, making it easier for users to keep up with relevant data.
- Announcements: Share information with the whole organization at once to ensure that everyone remains on the same page.
- Task Management: Create digital checklists to determine progress on vital tasks – or to keep up with your own responsibilities.

Principal Service Commitments and System Requirements

Pronto designs its processes and procedures to meet its objectives for its services. Those objectives are based on the service commitments that Pronto makes to user entities, the laws and regulations that govern the provisioning of services, and the financial, operational, and compliance requirements that Pronto has established for the services. Pronto's services are subject to privacy laws and regulations in the jurisdictions in which Pronto operates. Security commitments to user entities are documented and communicated in its Customer Data Security Policy and other customer agreements.

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

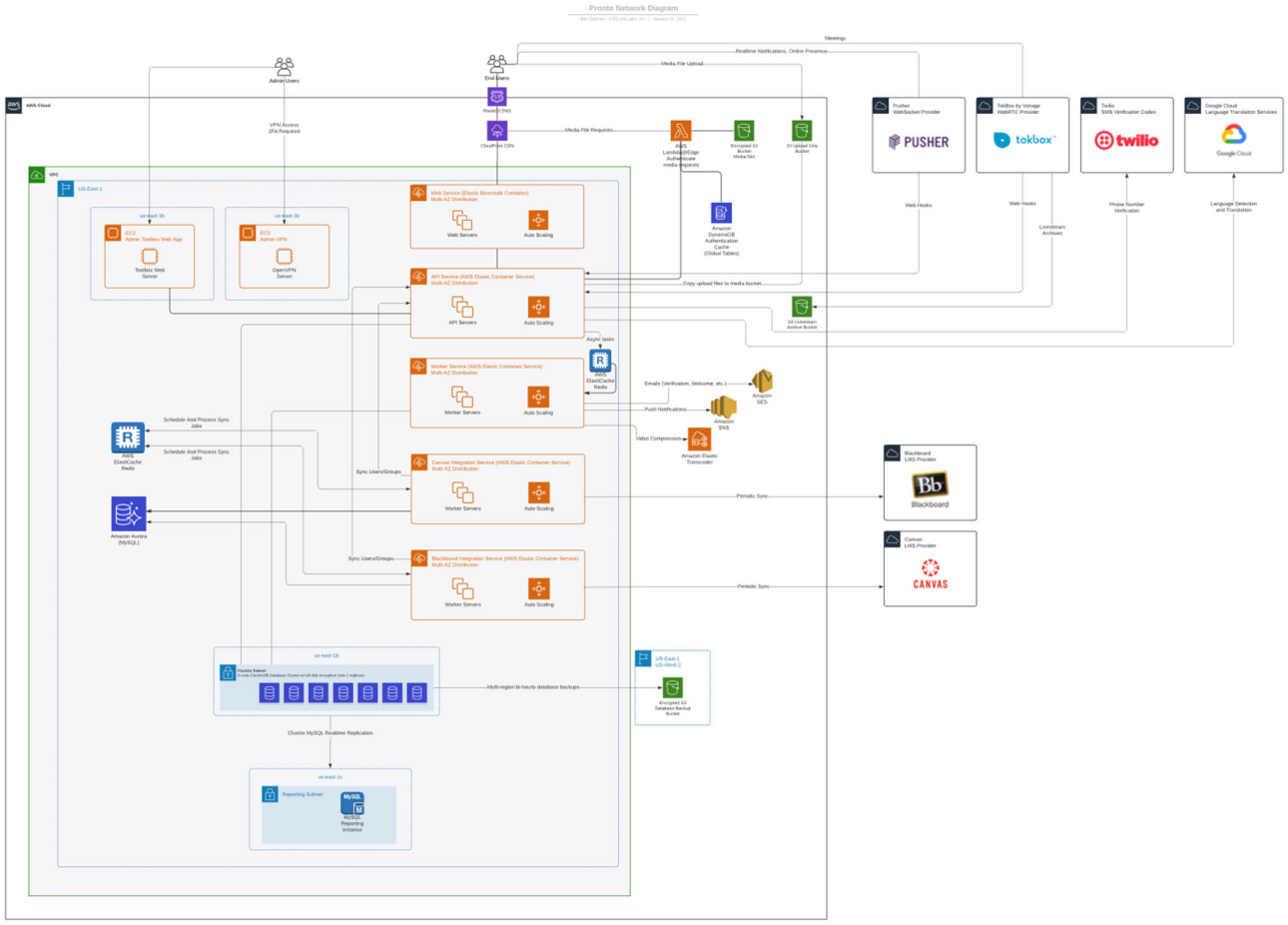
- Maintain reasonable administrative, physical, and technical safeguards designed to protect customer data, consistent with industry standards. Those safeguards include measures designed to prevent unauthorized access, acquisition, deletion, and disclosure of customer data by Pronto personnel.
- Before sharing customer data with a third-party service provider, Pronto will require that the third party maintains reasonable data practices designed to maintain the security of customer data and preventing unauthorized acquisition or use of the customer data.
- Notify customers of security incidents as expeditiously as possible upon becoming aware of such an event, with an official written report being delivered to customers within two weeks of the incident.

Pronto establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Pronto's system policies and procedures, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around system design, development, and operations, as well as management of internal business systems and networks. 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 Pronto's system.

Components of the System

Infrastructure

Pronto operates a cloud-based network within Amazon Web Services (AWS), which provides secure hosting of network and production systems. The key infrastructure components are noted in the table below.



Component	Purpose
Elastic Load Balancers	Intelligently directs incoming web traffic to appropriate back-end services in ECS and Elastic Beanstalk.
Elastic Container Service	Container technology used to deploy and scale the Pronto API services
Elastic Beanstalk	Technology used to deploy and scale the Pronto Web services
Clustrix (a.k.a. XpandDB)	Database used for managing the customer data processing infrastructure
RDS MySQL Database	Database used for LTI integrations and reporting replicas
AWS EC2	Managed instances

Component	Purpose
AWS S3	Storage of customer audio, images, and documents
AWS Route53	DNS and domain registration
AWS Simple Email Service (SES)	SMTP server for sending emails to customers
AWS Simple Notification Service (SNS)	Service for sending push notifications to customers
AWS CloudWatch	Managed service for platform logging and operational alarms
Vonage (a.k.a. TokBox)	WebRTC platform that powers real-time video conferencing in Pronto
Twilio	Managed platform for sending SMS verification codes to customers
Google Cloud Translation API	Managed platform for translation of messages in Pronto
Pusher	Managed platform for WebSockets for real-time event updates

Software

Primary software used to support Pronto's Platform are noted in the table below.

Software	Purpose
Github	Source code repository and version control system
Google Workspace (Formerly GSuite)	Email, Document Management, User and Group Management
New Relic	Operations insight and metrics platform
AWS CloudWatch	Managed service provider for platform logging
Intercom	To handle customer support requests and provide customer documentation

People

Pronto maintains a staff of approximately 25 employees across the functional areas of executive management, engineering, product, sales and customer success, customer support, IT operations, general operations, human resources, and content and marketing.

Executive Management

The Executive Management team incorporates the following individuals:

- Chief Executive Officer (CEO)
- Chief Technology Officer (CTO)
- Chief Revenue Officer (CRO)
- Vice President of Customer Success
- Head of Marketing

Executive Management is responsible for developing and implementing strategic initiatives, addressing legal/ regulatory requirements, and overseeing their respective teams.

Operations

The Senior Director of Operations together with the respective operations teams oversee general and sales operations and data and analytics for the Company.

Finance & Legal

The Chief Executive Officer and the finance team oversee accounting, board governance, financial planning & analysis, tax, accounts payable and receivable operations, legal, investment, and funding activities.

Human Resources

The Human Resources Manager and the people team are responsible for maximizing employee value to the Company through talent acquisition, employee onboarding, talent management, benefits, employee engagement, employee experience and culture, and internal communications.

Engineering and Technology

The Chief Technology Officer oversees engineering, product management, and information security. Engineering builds and designs applications, back-end infrastructure for all products, and customer deliverables. The development team coordinates and implements the building and delivery of the Company's products.

Product

The Senior Director of Product and the product team are responsible for ensuring that the Company's strategy is realized through the delivery of software solutions to waiting markets, while taking into account the needs of customers and end users using the products.

Sales and Customer Success

The Chief Revenue Officer oversees all direct sales activities and sales operations. The Account Executives that make up the sales team conduct outbound emailing, calling, and networking activities to generate new net customers for the Company as well as upsell to current customers. The teams provide the technology foundation for coordinating these outbound activities.

The Customer Success Managers that make up the customer success team conduct new customer onboarding, renewal activities, and maintain existing customer accounts.

Marketing

The Head of Marketing and the content and marketing team are responsible for all promotional activities for the Company and its products through various digital and non-digital channels, including website and search optimization, email and database marketing, social media, PR, webinars, and conferences. The team develops content and manages the distribution of messaging to target markets to support the Company's commercial objectives.

Data

Pronto classifies data based on the degree of confidentiality required using the following labels:

- **Unrestricted** - data will be classified as unrestricted when the unauthorized disclosure, alteration or destruction of that information would result in little or no risk to the Company and its affiliates.
- **Confidential** - by default, all customer data that is not explicitly classified as Restricted or Unrestricted will be treated as Confidential. Personal data such as an email address is classified Confidential.
- **Restricted** - data protected by legislation and/or confidentiality agreements. The highest level of security controls will be applied.

A classification of an item of information may change over time.

Any data file or printed document that is not labeled and contains sensitive data is considered classified as "Confidential" and handled accordingly.

Within Pronto's AWS cloud-based environment, confidential data is stored encrypted in MySQL and Clustrix databases. Access to the data is only available via the user's web browser or mobile device by authenticating to and using the Pronto application. It requires an authenticated user session and proper authorization profile in the system. The access to such data only for authorized users is validated at least once a year through penetration testing performed by an independent vendor. All such customer's data is considered confidential.

Procedures

The following security policies and procedures are maintained and updated at least annually by Pronto:

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity & Disaster Recovery Plan
- Change Management Policy
- Code of Conduct Policy
- Cryptography Policy
- Data Classification Policy
- Data Deletion Policy
- Incident Response Plan
- Information Security Policy
- Password Policy
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Program
- System Access Control Policy
- Vendor Management Policy
- Vulnerability Management Policy

Pronto employees and contractors are required to read all applicable Company policies and document their understanding and acknowledgement of specific policies and procedures upon hire and on an annual basis.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Control Environment

Management's Philosophy

Integrity and ethical values are essential elements of management's philosophy and Pronto's control environment. The executive team is responsible for setting the example of ethical conduct at Pronto and communicating expectations across the organization through the Code of Conduct policy.

Security Management

Pronto has a cross-functional information security working group consisting of the CTO, CEO, DevOps Engineer, and several other engineers.

The CTO is designated as the Information Security Officer at Pronto and is responsible for creating and enforcing security policies and procedures, leading the monitoring, vulnerability management, incident detection and response initiatives, and minimizing risk across the organization.

All Pronto employees are required to attend information security awareness training on an annual basis to ensure that personnel are knowledgeable of risks and controls around cybersecurity and data protection.

Personnel Security

New positions that are posted at Pronto have clearly defined job descriptions and outline the technical and educational requirements the Company is seeking in prospective candidates. Background checks are performed on new employees prior to their start date. Once employed, personnel are subject to Pronto's procedures around information security. A provisioning ticket is submitted to the IT team requesting that the newly hired employee or contractor obtain the system access necessary to perform their job. Access is granted based on the principle of least privilege.

Personnel Security

New positions that are posted at Pronto have clearly defined job descriptions and outline the technical and educational requirements the Company is seeking in prospective candidates. Background checks are performed on new employees prior to their start date. Once employed, personnel are subject to Pronto's procedures around information security. A provisioning ticket is submitted to the IT team requesting that the newly hired employee or contractor obtain the system access necessary to perform their job. Access is granted based on the principle of least privilege.

Physical Security and Environmental Controls

The in-scope systems and infrastructure that support Pronto are hosted in the cloud by AWS (see *Complementary Subservice Organization Controls* section below). Pronto's Physical Security Policy outlines requirements around securing the office and Company equipment and includes disciplinary actions for those who violate the policy.

Logical Security

Pronto 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.

Employees and approved vendor personnel sign on to the Pronto production network using secure credentials, which includes two-factor authentication. Passwords must conform to defined password standards established in the Password Policy and are enforced through parameter settings where possible.

All employees accessing the production system, whether from outside the Pronto offices or inside, are required to use a token-based two-factor authentication system. Customer systems access the Pronto customer portal through the Internet using HTTPS. In all cases, connections must use protocols that encrypt passwords before they will fully function.

Employees of Pronto customers access Pronto services through the Internet using the SSL functionality of their web browser. Users must either supply a valid user ID and password with two-factor authentication or use OAuth via Google to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured in the Pronto console by the administration account.

Change Management

Pronto 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. Code review and exploratory testing results are documented and maintained with the associated pull request which is linked to the change request. Development and testing are performed in an environment that is entirely separate from 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.

System Monitoring

Pronto management performs system monitoring activities to continuously assess the quality of internal control over time and ensure that any corrective actions are completed in a timely manner. Examples of system monitoring processes in place include:

- Firewalls – Systems that filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.
- Vulnerability Scanning – Daily process by which infrastructure and software is automatically tested for security weaknesses.
- Patch Management – Ensures contacted customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches.
- Penetration Testing – External network and authenticated / unauthenticated web application penetration testing to identify, and subsequently remediate, vulnerabilities that can be exploited by bad actors.

Problem Management

Security incidents and other IT-related issues are reported to the CTO. Issues are tracked using the Company's ticketing system and are monitored to ensure timely resolution.

Data Backup and Recovery

Product-specific customer data and end user data is backed up and monitored by engineering personnel. Sales and marketing data is backed up and monitored for completion and exceptions by operations personnel. 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 depending on customer indicated preference within the documented work instructions.

Backup data is stored remotely with AWS, where no Pronto personnel have any physical access.

An incident response policy 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.

Risk Assessment Process

Pronto conducts an enterprise risk assessment at least annually. The system risk assessment template enables Pronto to categorize risks to the business, describe their cause and potential impact, and outline mitigation steps to reduce the likelihood and impact. From there, Pronto assigns a likelihood and impact rating to the risk statement and determines whether to accept the risk or to apply additional mitigation strategies.

Information and Communication Systems

Information and communication is an integral component of Pronto's 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 Pronto, information is identified, captured, processed, and reported by various information systems as well as through conversations with customers, suppliers, regulators, contractors, 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. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Pronto personnel via company-wide web calls, Pronto, and e-mail messages.

Monitoring Controls

Pronto's management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Pronto 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 Pronto's policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Ongoing Monitoring

Pronto's 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 Pronto's 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 Pronto's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Pronto personnel.

Reporting Deficiencies

Pronto's risk and issues register 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 and/or issues. Live issues followed by risks receiving a high rating are responded to immediately. Corrective actions are documented and tracked within the risk and issues register. Regular risk meetings are held for management to review reported deficiencies and corrective actions.

Control Objectives and Related Controls

Pronto's control objectives and description of related controls are included in Section IV, 'Trust Services Categories, Criteria, and Related Controls Relevant to Security'. Although the control objectives and related controls are included in Section IV, they are an integral part of the description of the system.

Complementary User Entity Controls (CUECs)

Pronto's controls cover only a portion of overall internal control for each user entity of the communication system. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Pronto. Therefore, each user entity's internal control should be evaluated in conjunction with Pronto's controls, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

Criteria	Control Activity
CC6.1	User entities are responsible for using commercially reasonable efforts to prevent unauthorized access to, or use of, the Pronto communication system and for notifying the Company promptly of any such unauthorized access of use.

Complementary Subservice Organization Controls (CSOCs)

Pronto utilizes the following subservice organization:

- AWS, a subsidiary of Amazon that provides on-demand cloud computing platforms to individuals, companies, and governments, on a paid subscription basis. The technology allows subscribers to have at their disposal a virtual cluster of computers, available all the time, through the Internet.

Pronto's services are designed with the assumption that certain controls will be implemented at AWS. Such controls are called complementary subservice organization controls. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Pronto. Therefore, each user entity's internal control must be evaluated in conjunction with Pronto's controls, considering the related CSOCs expected to be implemented at the subservice organization, as described below.

Criteria	Control Activity
CC6.4	• AWS is responsible for restricting data center access to authorized personnel. • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC9.1	• AWS is responsible for the installation of fire suppression, detection, and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterrupted power supply. • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Pronto receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Pronto monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Pronto also has communication with the subservice organization to monitor compliance with the service agreement, stay up to date on planned changes at the hosting facility, and communicate any issues or concerns to AWS management.

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure to the achievement of one or more of those service commitments and system requirements as of May 31, 2022.

Trust Services Criteria Not Applicable

All criteria within the security category were applicable to the communication system.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service as of May 31, 2022.

Report Use

The description does not omit or distort information relevant to the system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not therefore include every aspect of the system that each individual user may consider important to his or her own particular needs.

SECTION IV

TRUST SERVICES CATEGORIES, CRITERIA, AND RELATED CONTROLS RELEVANT TO SECURITY

SECURITY

Control #	Control Activity Specified by Pronto
Control Environment	
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	Hit Labs, Inc. ('Pronto' or 'the Company') has established a Code of Conduct policy that is acknowledged by all new employees and contractors upon hire. This policy outlines expectations the Company has set related to ethics and standards of conduct. Additionally, this policy outlines processes that Management has established to evaluate adherence to standards of conduct and address deviations in a timely manner.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	Pronto has a Board of Directors that is made up of independent leaders with relevant skills and industry expertise, which enables them to provide credible challenge and oversight over management.
CC1.2.2	On a quarterly basis, Management and the Board of Directors meet to discuss Company performance, strategic objectives, and information security matters.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	Pronto maintains an updated organizational chart that establishes structure, reporting lines, and delegation of authority and responsibility across the Company.
CC1.3.2	Pronto has an assigned security team that is responsible for the design, implementation, and oversight of the organization's security policies and procedures. The security team communicates important information security events to Management in a timely manner.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	All positions have a detailed job description that lists qualifications, such as required skills and experience, which candidates must meet in order to be hired by Pronto.
CC1.4.2	Background checks are performed on new hires for select high-risk positions before the new hire's start date, as permitted by local laws. These positions include those on the executive team, executive assistants, and roles pertaining to physical and information security. The results of the background checks are reviewed by HR and appropriate action is taken if deemed necessary.
CC1.4.3	On a quarterly basis, Management and the Board of Directors review the competency of its staff against the required business objectives and forecasted growth to determine whether additional resources are necessary.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	Pronto maintains formalized performance expectations for each position and uses these expectations as a basis for evaluating the performance of each of its employees. These performance evaluations, which incorporate internal control responsibilities, are completed on an annual basis.

Control #	Control Activity Specified by Pronto
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.	
CC2.1.1	Pronto's mission-critical systems and sensitive information are identified during the annual risk assessment, which includes capturing internal and external sources of data.
CC2.1.2	Pronto maintains an updated network diagram outlining how data is processed and secured.
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.	
CC2.2.1	Pronto maintains updated policies and procedures that enable all personnel to understand and carry out their internal control responsibilities. These policies and procedures are accessible to all personnel and are acknowledged upon hire and on an annual basis.
CC2.2.2	Pronto employees and contractors are required to complete an annual information security awareness training.
CC2.2.3	Pronto provides a process for employees and contractors to report security, confidentiality, integrity and availability failures, incidents, and concerns and other complaints to Management.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	Pronto maintains an updated Privacy Policy on its website that communicates the Company's commitment to privacy to external users. The policy provides a contact method for questions or complaints.
CC2.3.2	Pronto enables inbound communications from customers and other stakeholders by maintaining contact information on their website for general inquiries, customer support, partnerships, and public relations.
CC2.3.3	Objective descriptions of Pronto's system and its boundaries are available to authorized external users and customers.
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.	
CC3.1.1	Pronto maintains an updated Risk Assessment Program that describes the processes the Company has in place to identify new business and technical risks and how those risks are mitigated.
CC3.1.2	At least annually, Pronto conducts an assessment on the risks related to operations, regulatory compliance, information security, physical security, and fraud.
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.	
CC3.2.1	At least annually, Pronto performs a risk assessment, which includes the identification of relevant internal and external threats, an analysis of the significance of the risks associated with those threats, a determination of appropriate risk mitigation strategies, and the development or modification of controls consistent with the risk mitigation strategy.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	As part of the risk assessment process, Management conducts a fraud assessment that considers various types of fraud exposure, along with incentives / pressures, opportunities, and rationalizations that could be present.

Control #	Control Activity Specified by Pronto
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	As part of the risk assessment process, Management identifies and assesses changes that could significantly impact the system of internal control. The assessment includes evaluating changes in the external environment, regulations, business model, leadership, IT, and vendor / business partner relationships.
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.	
CC4.1.1	Pronto conducts ongoing monitoring over internal controls to ensure they are appropriately designed and operating effectively in accordance with baseline requirements. These evaluations are conducted with knowledgeable personnel, integrate with business processes, consider changes in business processes, and vary in frequency based on associated risks.
CC4.1.2	Pronto engages a qualified third-party security firm to conduct web application penetration tests at least annually. Results are reviewed by management and high priority findings are remediated in a timely manner.
CC4.1.3	Intrusion prevention and detection systems are used to provide continuous monitoring of the Company's network and to protect against potential security breaches.
CC4.1.4	Pronto has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in the Company's infrastructure.
CC4.1.5	Pronto has established a formalized phishing prevention and monitoring campaign to evaluate employee compliance with the information security policy related to phishing.
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 board of directors, as appropriate.	
CC4.2.1	Management assesses the results of ongoing and separate evaluations. Deficiencies are communicated to relevant parties for corrective action and Management tracks whether the deficiencies are remediated in a timely manner.
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.	
CC5.1.1	As part of the risk assessment process, Management ensures that adequate controls are in place to mitigate the identified risks to an acceptable level. Considerations in the identification and implementation of control activities include entity-specific factors, relevant business processes, incorporating a mix of control activity types (manual, automated, preventive detective) and segregation of duties.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	Pronto maintains a suite of Information Technology General Controls (ITGCs) to support the achievement of objectives. These ITGCs are identified as part of the annual risk assessment completed by Management and cover areas such as technology infrastructure and security management, as well as technology acquisition, development, and maintenance.
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.	
CC5.3.1	Pronto maintains updated policies and procedures that incorporate control activities across the organization. These policies and procedures establish requirements pertaining to timely performance of controls, taking corrective action on control deficiencies, and ensuring that competent personnel are accountable for control execution.

Control #	Control Activity Specified by Pronto
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.	
CC6.1.1	Pronto maintains an updated inventory of information assets within the organization.
CC6.1.2	Access to Pronto's critical systems and applications requires complex passwords and multi-factor authentication (MFA).
CC6.1.3	Pronto utilizes Virtual Private Clouds (VPCs) and sub-networks (subnets) to achieve network segmentation in its AWS cloud-based environment.
CC6.1.4	Pronto utilizes password managers to store encrypted passwords in the cloud.
CC6.1.5	Pronto utilizes identity and access management tools within AWS to securely manage access to services and resources.
CC6.1.6	Pronto encrypts data at-rest through server-side encryption (SSE) using AES-256.
CC6.1.7	Pronto maintains active SHA-256 encryption certificates for its web application to ensure secure connections for its users.
CC6.1.8	Pronto encrypts all employee and contractor workstations with full disk encryption.
CC6.1.9	Pronto creates and manages cryptographic keys and controls their use.
CC6.1.10	Pronto maintains a secure administrator account that manages the system. Administrative rights are granted only to individuals who require access to fulfill their job responsibilities.
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.	
CC6.2.1	The IT department approves system access for newly hired personnel as well as access change requests.
CC6.2.2	System access is removed within 24 hours upon employee or contractor termination.
CC6.2.3	On at least a quarterly basis, the CTO reviews access rights for all Pronto employees to ensure that system access is appropriate. Any access rights that are no longer needed are removed following this review.
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.	
CC6.3.1	The IT department approves system access for newly hired personnel as well as access change requests.
CC6.3.2	System access is removed within 24 hours upon employee or contractor termination.
CC6.3.3	On at least a quarterly basis, the CTO reviews access rights for all Pronto employees to ensure that system access is appropriate. Any access rights that are no longer needed are removed following this review.
CC6.3.4	Pronto maintains remote-wipe software in the event of loss / theft of Company workstations.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
Pronto does not currently have a physical office space (all employees are remote, home-based). Additionally, Pronto uses AWS for cloud computing and data center hosting services. Please reference *Complementary Subservice Organization Controls (CSOCs)* in Section III for additional controls that are to be implemented by the subservice organization.	

Control #	Control Activity Specified by Pronto
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read and recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.5.1	Pronto has a data handling and disposal policy that governs how different types of data are retained and deleted.
CC6.5.2	Prior to disposing of obsolete workstations or removable media, the IT department ensures that all physical devices are sanitized to remove any confidential information.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	Firewall rules are configured to restrict network traffic to approved ports, protocols, and sources.
CC6.6.2	Pronto utilizes a web application firewall (WAF) to protect the Pronto platform from web-based threats.
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.	
CC6.7.1	Pronto utilizes a virtual private network (VPN) to enable secure remote access for its employees and contractors.
CC6.7.2	Data in-transit is protected through secure (authenticated and encrypted) industry accepted standardized network protocols.
CC6.7.3	A centralized mobile device management (MDM) solution has been deployed to all mobile devices to enforce password complexity requirements and auto-locks for failed login attempts.
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.	
CC6.8.1	Pronto utilizes endpoint protection software to prevent and detect unauthorized or malicious software such as viruses, malware, and ransomware. Alerts, logs, and reports are generated when potential threats are detected.
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.	
CC7.1.1	Pronto maintains updated baseline configurations for its information systems and system components to reflect the current enterprise architecture.
CC7.1.2	Pronto utilizes Amazon GuardDuty as a threat detection service that continuously monitors for malicious activity and unauthorized behavior related to AWS accounts, workloads, and data.
CC7.1.3	Pronto conducts automated vulnerability scanning on a continuous basis.
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.	
CC7.2.1	Pronto maintains updated detection policies, procedures, and tools to identify anomalies or unusual activity on information systems. Potential security incidents are filtered and analyzed based on established detection measures.
CC7.2.2	Detection tools are periodically analyzed by management for effectiveness, and remedial action is taken when necessary.

Control #	Control Activity Specified by Pronto
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.	
CC7.3.1	Pronto has established an internal ticketing system for tracking potential incidents. Tickets are prioritized based on their impact and severity.
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.	
CC7.4.1	Pronto maintains an updated incident response program, establishes roles and responsibilities, and includes procedures for containing, mitigating, and ending the threats posed by security incidents, as well as restoring operations and communicating security incidents and actions taken to affected parties.
CC7.4.2	Pronto follows the incident response program by understanding the nature of the incident, determining a containment strategy, remediating identified vulnerabilities and communicating remediation activities.
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	Pronto follows the incident response program to restore the affected environment to full operation by rebuilding systems, updating software, installing patches, and/or changing configurations, as needed.
CC7.5.2	Information about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events is communicated to management and other internal and external parties, as appropriate.
CC7.5.3	After an incident has been resolved and appropriate parties have been notified, a postmortem that includes a root cause analysis and lessons learned is completed. Architectural and/or procedures changes are implemented, when possible, to prevent and detect recurrences of similar incidents. This includes conducting additional training to educate personnel on how to prevent future incidents.
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.	
CC8.1.1	Pronto maintains an updated Change Management Policy that governs the software development lifecycle (SDLC), including (1) authorizing system changes prior to development; (2) designing and developing system changes; (3) documenting and tracking changes prior to implementation; (4) testing and approving system changes; (5) deploying changes to production; (6) evaluating the changes against their objectives; and (7) modifying infrastructure, data, software and procedures to remediate identified incidents.
CC8.1.2	Pronto uses a version control system to manage source code, documentation, release labeling, and other change management tasks.
CC8.1.3	Engineers who make changes to the development system are unable to deploy those changes to production without independent approval.
CC8.1.4	Changes to the production environment are communicated to affected internal and external stakeholders.
Risk Mitigation	
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	Pronto maintains insurance to mitigate the financial impact of business disruptions, including cyber incidents.
CC9.1.2	Pronto maintains an updated Business Continuity and Disaster Recovery Plan that guides the organization in how to respond and recover from disruptions in networks, systems, and internal operations.
Pronto uses AWS for cloud computing and data center hosting services. Please reference *Complementary Subservice Organization Controls (CSOCs)* in Section III for additional controls that are to be implemented by the subservice organization.	

Control #	Control Activity Specified by Pronto
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	Pronto maintains an updated Vendor Management Policy to monitor and ensure service levels and ongoing compliance of existing vendors and third parties.
CC9.2.2	Pronto conducts comprehensive vendor due diligence prior to onboarding a new vendor, as well as on an annual basis for existing vendors. This includes performing a vendor risk assessment and reviewing the SOC 2 reports, ISO 27001 certifications, and/or responses to information security questionnaires.