REDFISH LABS, INC. DBA TORCH LEADERSHIP LABS

Torch Platform

SOC 3

System and Organization Controls (SOC) for Service Organizations Report for the period of October 1, 2024 to September 30, 2025

Aprio®

Passionate for what's next®

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined Redfish Labs, Inc. DBA Torch Leadership Labs (the "Company" or "Torch") accompanying assertion titled *Redfish Labs, Inc. DBA Torch Leadership Labs' Assertion* (the "Assertion") indicating that the controls within the Torch Platform (the "System") were effective for the period of October 1, 2024 to September 30, 2025 (the "Specified Period") to provide reasonable assurance that Torch's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*) for the Specified Period.

The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Amazon Relational Database Service (RDS) and AWS Simple Storage Service (S3) as a Database-as-a-Service. Additionally, the Company uses Altimetrik Corp. as a third-party company that provides contractors to Torch, including completion of background checks, security awareness training, and policy acknowledgments for all contractors prior to employment. Certain AICPA applicable trust services criteria specified in the section titled *Redfish Labs, Inc. DBA Torch Leadership Labs' Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion does not disclose the actual controls at the subservice organizations. 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.

Service Organization's responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Redfish Labs, Inc. DBA Torch Leadership Labs' Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that the controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria;
- performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria;
- performing procedures to obtain evidence about whether controls were suitably designed and operating effectively to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- testing the operating effectiveness of controls to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

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

Service Auditor's independence and quality control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA issued by the International Ethics Standards Board for Accountants (IESBA Code). We have applied the Statements on Quality Control Standards established by the AICPA and, accordingly, have designed, implemented, and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other matters

We did not perform any procedures and accordingly do not express an opinion on the description in Section III titled *Redfish Labs, Inc. DBA Torch Leadership Labs' Description of the Boundaries of its System.*

Opinion

In our opinion, Torch's assertion that the controls within the Company's System were effective for the period October 1, 2024 to September 30, 2025 to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects, is fairly stated.

Aprio, LLP

Aprio, LLP

Atlanta, Georgia
November 3, 2025

II. Redfish Labs, Inc. DBA Torch Leadership Labs' Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Redfish Labs, Inc. DBA Torch Leadership Labs' (the "Company" or "Torch") Torch Platform (the "System") for the period of October 1, 2024 to September 30, 2025 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, Confidentiality, and Privacy were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (the "applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*). The Company's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. Our description of the boundaries of the system and principal service commitments and system requirements related to the applicable trust services criteria are specified in the section titled *Redfish Labs, Inc. DBA Torch Leadership Labs' Description of the Boundaries of its System*.

The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Amazon Relational Database Service (RDS) and AWS Simple Storage Service (S3) as a Database-as-a-Service. Additionally, the Company uses Altimetrik Corp. as a third-party company that provides contractors to Torch, including completion of background checks, security awareness training, and policy acknowledgments for all contractors prior to employment. Certain AICPA applicable trust services criteria specified in the section titled *Redfish Labs, Inc. DBA Torch Leadership Labs' Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

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

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Redfish Labs, Inc. DBA Torch Leadership Labs' Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Redfish Labs, Inc. DBA Torch Leadership Labs's (the "Company" or "Torch") as it relates to its Torch Platform (the "System") for the period of October 1, 2024 to September 30, 2025 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Torch was founded in late 2017 in San Francisco, CA. Torch has fewer than 100 employees and is a fully remote company with a presence in San Francisco, CA. Torch is a leadership coaching solution which matches employees with a coach and gives them tools to guide them through their engagement. These tools include session scheduling, goal setting, 360 feedback assessments as well as learning and development capabilities.

The vision at Torch is to create the first software platform that merges cutting edge technology, human coaching, and mentorship aimed at creating high caliber leaders at all levels of Torch, ultimately driving innovation, scale, and the bottom line.

Torch empowers leaders to evolve in a fast-changing world through personalized coaching and technology. Torch's vision is to redefine leadership by developing leaders who inspire, collaborate, and drive change with empathy and resilience via 1:1, group and team coaching. Torch's mission is to unlock individual and organizational potential through deep connections, tailored coaching, and practical solutions that lead to meaningful and lasting impact.

Torch facilitates a holistic product design lifecycle helping to ensure complete transparency, clarity, and alignment with its internal teams, partners, and customers resulting in decreased risk and increased efficiency, productivity, quality, value, and trust. Torch succeeds by being extremely focused on delivering compelling, scalable, intentional end-to-end solutions for the problems of its customers and their employees. Torch's platform enables Employee, Team, and Organization - Engagement » Insight » Action » Growth.

C. System Overview

Supporting Systems Overview

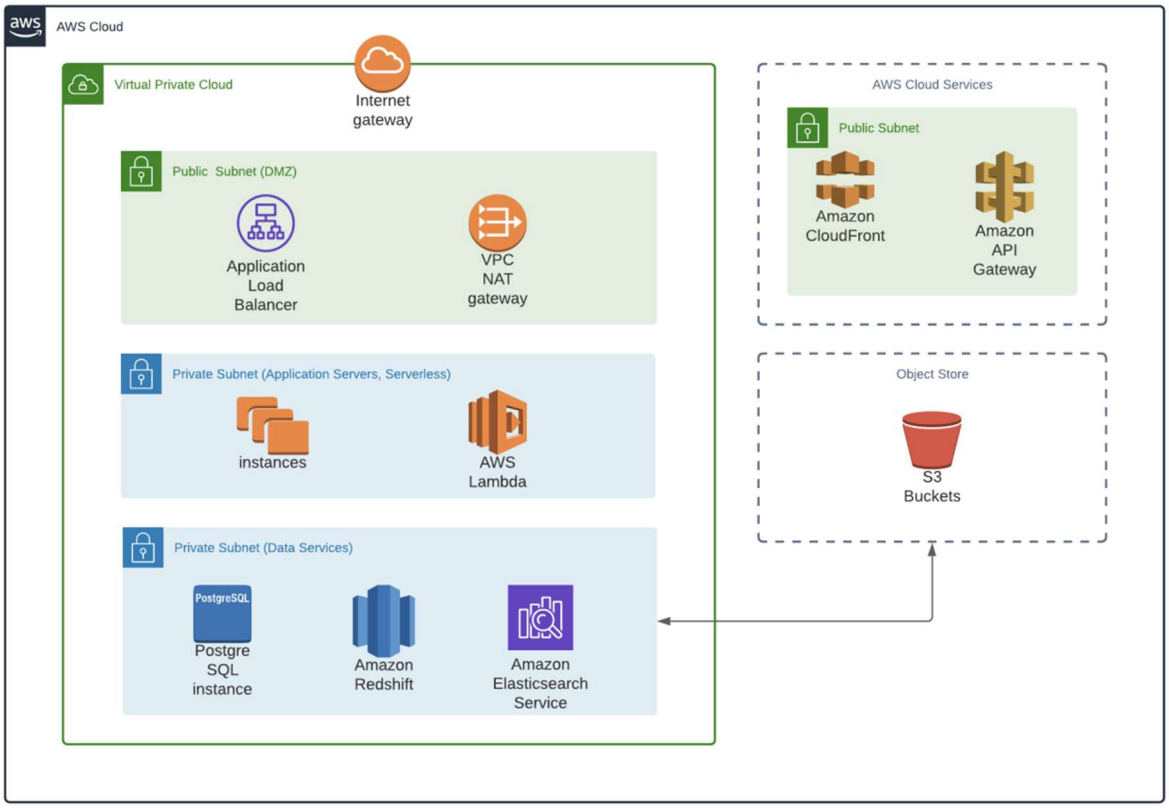
Torch's application network and infrastructure completely resides within Amazon Web Services (AWS). Internet-facing surface area is limited. Torch's application is a multi-tenant communication and learning platform.

1. Infrastructure and Databases

Network Overview

- The Torch System is a web application implemented using the React framework. The web front-end and other static assets are served using a CDN, AWS CloudFront.

- Data requests are handled by APIs implemented using both serverless, via Python, and a server-based Ruby on Rails-based framework.
- Access to publicly exposed endpoints is only permitted in designated network DMZs.
- Application servers, serverless functions, and databases are all located in private subnets with no direct access to the public internet. Limited subnet routing and deny-first security group rules help to ensure that network traffic and access is limited to services on an as-needed basis.
- All infrastructure is hosted in the AWS us-west-2 region.
- The Torch Platform runs on managed Kubernetes using the AWS Bottlerocket OS, designed specifically for security of containerized applications.



Systems Overview	Purpose
AWS EC2	System Infrastructure
AWS RDS for PostgreSQL	Database
AWS S3	Database
AWS Redshift	Data warehousing
AWS EKS Bottlerocket	Linux operating system to run AWS EKS containers
AWS CloudFront	System Infrastructure
G Suite	Single sign-on (SSO) tool
AWS Key Management Service (KMS)	Key management

D. Principal Service Commitments and System Requirements

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

- The use of security and confidentiality principles 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;
- The use of encryption technologies to protect customer data in transit over untrusted networks;
- The use of reasonable precautions to protect the security and confidentiality of the information that is collected;
- The use of availability principles that are designed to help ensure availability of the systems supporting the Torch System;
- Efforts to help ensure controls are in place to automatically remove certain personal information from the System;
- Efforts to destroy or encrypt any information that is not filtered automatically; and
- Efforts to collect, use, retain, disclose, and dispose of personal information to achieve Torch's service commitments and system requirements.

Torch establishes operational requirements that support the achievement of security, availability, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Torch's 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.

E. Non-Applicable Trust Services Criteria

Security, Availability, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**Torch's Rationale**
CC 6.4	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.	N/A – The Company's hosting provider, Amazon Web Services (AWS), is responsible for physical security controls. The Company does not maintain any hard copy data or store any customer information physically.
P 3.1	Personal information is collected consistent with the entity's objectives related to privacy.	N/A - The Company does not validate collected personal information for the Data Subject. The Data Subject is responsible for the accuracy and completeness of all personal information input into the applications.

Security, Availability, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**Torch's Rationale**
P 5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	N/A - The Data Subject is responsible for correcting and/or updating personal information. The Company is not responsible for the accuracy of the information created by the users in the system.
P 6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	N/A - The Company does not disclose personal information to third parties.
P 6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	N/A - The Company does not disclose personal information to third parties.
P 6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	N/A - The Data Subject is responsible for correcting and/or updating personal information. The Company is not responsible for the accuracy of the information created by the users in the system.
P 7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	N/A - The Data Subject is responsible for correcting and/or updating personal information. The Company is not responsible for the accuracy of the information created by the users in the system.

F. Subservice Organizations

The Company utilizes a subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services	The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Amazon Relational Database Service (Amazon RDS), AWS Simple Storage Service (S3), and AWS Key Management Services (KMS) as a Platform-as-a-Service, more specifically a Database-as-a-Service. Amazon S3 provides object storage through a web service interface. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; • Controls over the configuration settings within the EC2 instance to help ensure that data is encrypted and stored as per the configuration settings selected with AWS; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components for Amazon RDS, S3, and KMS such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over Amazon RDS, S3, and KMS including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls over AWS S3 redundancy, including controls over data replication; and • Controls around the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform RDS, S3, and KMS components as applicable. In addition, the Company has identified the following control activities to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* P 4.2* P 4.3* P 6.6*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary; • Data restore testing is performed on at least an annual basis to verify the integrity of the backup data; and • The Torch production environments are monitored by Datadog for uptime, latency, utilization, and active services on an ongoing basis, and IT personnel are automatically notified in the event of an incident.	
Altimetrik	The Company uses Altimetrik Corp. as a third-party company that provides contractors to Torch, including completing background checks, security awareness training, and policy acknowledgments for all contractors prior to employment. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the performance of background checks on contractors in compliance with local laws and regulations; • Controls around the performance of security awareness training for contractors; and • Controls around the performance of policy acknowledgments for contractors. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	CC 1.1* CC 1.4* CC 2.2*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at these subservice organizations that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. User Entity Responsibilities

Each user entity must evaluate its own system of internal controls for effective risk management and compliance. The internal controls described in this report occur at and are managed by the Company and only cover a portion of a comprehensive internal control structure relevant to a user entity. Each user entity must address the various aspects of internal control that may be unique to its particular organization. This section highlights those portions of the internal control structure that user entities have responsibility to develop and maintain but should not affect the ability of the Company to achieve its service commitments and system requirements.

Related Control Area	User Entity Responsibilities
Access	• User Entities leveraging SSO are responsible implementing controls for ensuring that access for users of the applications is removed timely. • User Entities not leveraging SSO are responsible for implementing controls for communicating to Torch when users of the applications should be removed and/or disabled. • User Entities leveraging SSO are responsible for implementing controls for ensuring that the password parameters meet their corporate standards. • User Entities not leveraging SSO are responsible for implementing controls for providing valid usernames and emails to accurately provide the user an email invite. • The User Entities are responsible for implementing controls for determining the user setup options for the applications.


Aprio