



# REDFISH LABS, INC. DBA TORCH LEADERSHIP LABS

## Torch Platform

System and Organization Controls (SOC) for Service Organizations Report  
for the period of October 1, 2022, to September 30, 2023



Report of Independent Service Auditor issued by Aprio LLP

This report is intended solely for the information and use of the Company, user entities of the Company's System for the Specified Period, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators.

# Table of Contents

<b>I.</b>	<b>Report of Independent Service Auditor .....</b>	<b>1</b>
<b>II.</b>	<b>Redfish Labs, Inc. dba Torch Leadership Labs' Assertion .....</b>	<b>3</b>
<b>III.</b>	<b>Redfish Labs, Inc. dba Torch Leadership Labs' Description of the Boundaries of its System .....</b>	<b>4</b>
	A. Scope and Purpose of the Report.....	4
	B. Company Overview and Background.....	4
	C. System Overview .....	4
	D. Principal Service Commitments and System Requirements .....	6
	E. Non-Applicable Trust Services Criteria.....	7
	F. Subservice Organizations .....	7
	G. User Entity Controls .....	9

## 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, 2022 to September 30, 2023 (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* (AICPA, *Trust Services Criteria*).

The Company uses Amazon Web Services (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services 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 firewalls, routers, and servers. In addition, the Company also uses the Amazon Relational Database Service (Amazon RDS) and AWS Key Management Services (KMS) as a Platform-as-a-Service. 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 organization. The Assertion 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 Assertion indicates that 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 *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

### **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.

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; and
- 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.

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

### **Inherent limitations**

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

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

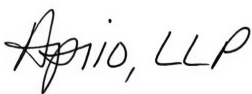
### **Other matters**

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *Company Name's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

### **Opinion**

In our opinion, Torch's assertion that the controls within the Company's 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, in all material respects, is fairly stated.

Aprio, LLP



Atlanta, Georgia  
November 8, 2023





## 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, 2022, to September 30, 2023 (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* (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. The 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*.

Torch uses Amazon Web Services (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services 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 firewalls, routers, and servers. In addition, the Company also uses the Amazon Relational Database Service (Amazon RDS) and AWS Key Management Services (KMS) as a Platform-as-a-Service. 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 organization.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Redfish Labs, Inc. dba Torch Leadership Labs' Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved only if complementary user entity controls contemplated 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 User Entities.

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 (the “Company” or “Torch”) as it relates to its Torch Platform (the “System”) for the period of October 1, 2022 to September 30, 2023 (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* (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. Currently, the Company has fewer than 200 employees and two offices (San Francisco, CA and Buffalo, NY). 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, social learning, and mentorship aimed at creating high caliber leaders at all levels of the company, ultimately driving innovation, scale, and the bottom line.

The Company 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. The Company succeeds by being focused on delivering scalable, intentional end-to-end solutions for the problems of its customers and their employees. The Company’s platform enables Employee, Team, and Organization - Engagement » Insight » Action » Growth.

### C. System Overview

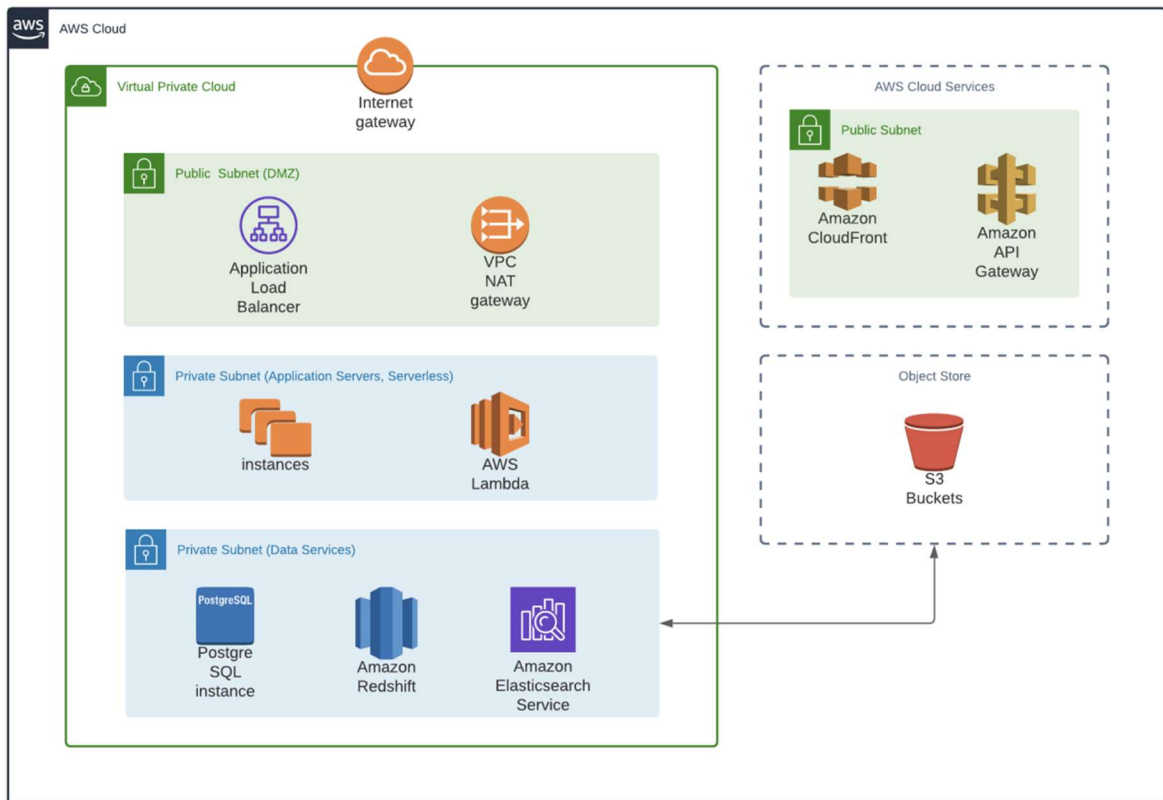
#### Infrastructure

Torch’s application network and infrastructure completely resides within Amazon Web Services (AWS). Internet facing surface area is extremely limited and consists of (cumulatively) only ports 22, 80, and 443. Torch’s application is a multi-tenant communication and learning platform.

#### 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 content delivery network (CDN) (AWS CloudFront).
- Data requests are handled by Application Programming Interfaces (APIs) implemented using both serverless with Python and ruby on rails-based framework with server-based framework (AWS API Gateway and Application Load Balancer, respectively).
- Access to publicly exposed endpoints is only permitted in designated networks (Demilitarized Zone [DMZs] and Amazon managed Cloud Services).

- Application servers, function calls (AWS Lambda), 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.



## Software

The following software tools are utilized in providing the Torch Platform services to user entities:

Name	Description
AWS	Cloud infrastructure services.
DataDog	Application logging.
Cronofy	G-Suite integration for session scheduling.
Twilio	Integrated video meeting services.
Atlassian	Customer support services.
Unbounce	Landing page optimization services.
StitchData	Advanced business analytics.
Postmark	End-user communications provider.

Name	Description
Sentry	Application logging.
Ziggeo	Integrated video recording services.
LogRocket	Application logging.
Zapier	System integration services.
Salesforce	Customer support services.
G-Suite	Facilitation of coach and user correspondence.
Preset	Advanced business analytics.
Cube	Advanced business analytics.
Airbyte	Advanced business analytics.
Tray.io	System Integration

#### 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;
- Make commercially reasonable efforts that controls are in place to automatically filter certain personal information collected from the System such as password and account numbers;
- Make commercially reasonable efforts that controls are in place to destroy or encrypt any information that is not filtered automatically; and
- Make commercially reasonable efforts to collect, use, retain, disclose, and dispose of personal information to achieve the Company'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 is protected.



### E. Non-Applicable Trust Services Criteria

Security, Availability, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		Redfish Lab, Inc. dba Torch Leadership Labs' 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.
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.
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.

### F. Subservice Organizations

The Company utilizes a subservice organization 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 organization described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at this subservice organization.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization 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 organization, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. 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 organization as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services	<p>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 firewalls, routers, and servers. The Company also uses the Amazon Relational Database Service (Amazon RDS) and AWS Key Management Services (KMS) as a Platform-as-a-Service. Amazon RDS is more specifically a Database-as-a-Service. The following control activities are critical to achieving the Applicable Trust Services Criteria:</p> <ul style="list-style-type: none"> <li>● 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;</li> <li>● Controls over managing infrastructure such as physical servers and physical access to backups and facilities;</li> <li>● Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform;</li> <li>● Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS;</li> <li>● Controls over incident monitoring, response, and follow up;</li> <li>● Controls over managing the Platform-as-a-Service components for Amazon RDS and KMS such as physical servers and operating systems including applying critical patching for this infrastructure;</li> <li>● Controls over Amazon RDS and KMS including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; and</li> <li>● Controls around the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform RDS and KMS components as applicable.</li> </ul> <p>In addition, the Company has identified the following control activity to help monitor the subservice organization:</p> <ul style="list-style-type: none"> <li>● 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</li> </ul>	<p>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 4.3*  P 6.6*</p>

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	<p>third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.</p> <ul style="list-style-type: none"> <li>Data restore testing is performed on at least an annual basis to verify the integrity of the backup data.</li> </ul>	

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

### G. User Entity Controls

Company Name's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary user entity controls identified within the table below, where applicable. As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
User Entities leveraging SSO are responsible for ensuring that access for users of the applications is removed timely.	CC 5.2* CC 6.2* CC 6.3*
User Entities not leveraging SSO are responsible for communicating to Torch when users of the applications should be removed and/or disabled.	CC 5.2* CC 6.3*
User Entities leveraging SSO should ensure that the password parameters meet their corporate standards.	CC 6.1*
For User Entities not leveraging SSO, the User Entities are responsible for providing valid usernames and emails to accurately provide the user an email invite.	CC 6.2*

User Entity Control	Associated Criteria
The User Entity is responsible for determining the user setup options for the applications.	CC 6.2* CC 6.3*

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

Aprio<sup>®</sup> 