



**A-LIGN**

Splashtop, Inc.

Type 2 SOC 3

2024



**SOC 3 FOR SERVICE ORGANIZATIONS REPORT**

**September 1, 2023 to August 31, 2024**

# Table of Contents

<b>SECTION 1 ASSERTION OF SPLASHTOP, INC. MANAGEMENT .....</b>	<b>1</b>
<b>SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT .....</b>	<b>3</b>
<b>SECTION 3 SPLASHTOP, INC.’S DESCRIPTION OF ITS REMOTE DESKTOP SERVICES SYSTEM THROUGHOUT THE PERIOD SEPTEMBER 1, 2023 TO AUGUST 31, 2024.....</b>	<b>7</b>
OVERVIEW OF OPERATIONS.....	8
Company Background .....	8
Description of Services Provided .....	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	12
Changes to the System Since the Last Review.....	13
Incidents Since the Last Review .....	13
Criteria Not Applicable to the System .....	13
Subservice Organizations.....	13
COMPLEMENTARY USER ENTITY CONTROLS.....	16

**SECTION 1**  
**ASSERTION OF SPLASHTOP, INC. MANAGEMENT**

## ASSERTION OF SPLASHTOP, INC. MANAGEMENT

September 13, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Splashtop, Inc.'s ('Splashtop' or 'the Company') Remote Desktop Services System throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Splashtop's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Splashtop, Inc.'s Description of Its Remote Desktop Services System throughout the period September 1, 2023 to August 31, 2024" and identifies the aspects of the system covered by our assertion.

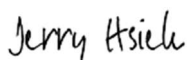
We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Splashtop's service commitments and system requirements were achieved based on the Trust Services Criteria. Splashtop's 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 presented in "Splashtop, Inc.'s Description of Its Remote Desktop Services System throughout the period September 1, 2023 to August 31, 2024".

Splashtop uses Amazon Web Services, Inc. (AWS), Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) to provide cloud hosting services, and Devo Technology Inc. (formerly LogicHub) (Devo) to provide security monitoring services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Splashtop, to achieve Splashtop's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Splashtop's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Splashtop's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Splashtop's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the applicable Trust Services Criteria and the complementary user entity controls assumed in the design of Splashtop's controls.

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 period September 1, 2023 to August 31, 2024 to provide reasonable assurance that Splashtop's service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Splashtop's controls operated effectively throughout that period.



---

Jerry Hsieh  
Vice President, Security and Compliance  
Splashtop, Inc.

**SECTION 2**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**



## INDEPENDENT SERVICE AUDITOR'S REPORT

To Splashtop, Inc.:

### *Scope*

We have examined Splashtop's ('Splashtop' or 'the Company') accompanying assertion titled "Assertion of Splashtop, Inc. Management" (assertion) that the controls within Splashtop's Remote Desktop Services System were effective throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Splashtop's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in *AICPA Trust Services Criteria*.

Splashtop uses AWS, GCP and OCI to provide cloud hosting services, and Devo to provide security monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Splashtop, to achieve Splashtop's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Splashtop's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Splashtop's controls. The description 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.

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

Splashtop 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 Splashtop's service commitments and system requirements were achieved. Splashtop has also provided the accompanying assertion (Splashtop assertion) about the effectiveness of controls within the system. When preparing its assertion, Splashtop 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 management's assertion that 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 AICPA. 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 description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether 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

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

#### *Independence and Ethical Responsibilities*

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*

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

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

#### *Opinion*

In our opinion, management's assertion that the controls within Splashtop's Remote Desktop Services System were suitably designed and operating effectively throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Splashtop's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Splashtop's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Splashtop's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.



*Restricted Use*

This report, is intended solely for the information and use of Splashtop, user entities of Splashtop's Remote Desktop Services during some or all of the period September 1, 2023 to August 31, 2024, business partners of Splashtop subject to risks arising from interactions with the Remote Desktop Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida  
September 13, 2024

## **SECTION 3**

### **SPLASHTOP, INC.'S DESCRIPTION OF ITS REMOTE DESKTOP SERVICES SYSTEM THROUGHOUT THE PERIOD SEPTEMBER 1, 2023 TO AUGUST 31, 2024**

## OVERVIEW OF OPERATIONS

### Company Background

Splashtop was founded in 2006 to provide remote access, remote support, cross-device productivity, and collaboration experience - bridging smartphones, tablets, computers, televisions, and clouds. The organization is headquartered in Cupertino, California with offices in Amsterdam, Tokyo, Singapore, Hangzhou and Taipei.

### Description of Services Provided

Splashtop provides remote access software that enables end users to remotely access and control remote computers, tablets, or smartphones.

Information Technology (IT) and helpdesks use Splashtop to remotely access their customer's systems to fix problems or provide training to end customers.

### Principal Service Commitments and System Requirements

Splashtop provides Software-as-a-Service (SaaS) which utilizes AWS, GCP, and OCI. This provides an infrastructure that is multi-cloud and cross-regional.

Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security concepts within the fundamental designs of the Task Management System (TMS) that are designed to permit system users to access the information needed based on their role in the system while restricting them from accessing information not needed for their role. Use of encryption technologies to protect customer data both at rest and in transit. Splashtop defines privacy requirements of user entities. Refer to [www.splashtop.com/privacy](http://www.splashtop.com/privacy)
- Splashtop establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Splashtop'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. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the TMS

## Components of the System

### Infrastructure

Primary infrastructure used to provide Splashtop's Remote Desktop Services System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
AWS Global Infrastructure	Cloud Hosting Services	Hosting the customer database, Application Programming Interface (API) servers, and relay servers for establishing remote connections
GCP and OCI	Cloud Hosting Services	Provide relay services
AWS, GCP, and OCI Instances	Linux	Provide remote desktop service over the Internet
AWS Containers	Kubernetes (Container Orchestration)	Hosting API. Provide remote desktop service over the Internet
AWS Web Application Firewall (WAF)	WAF	Application firewall
AWS Aurora	Database	Customer database

### Software

Primary software used to provide Splashtop's Remote Desktop Services System includes the following:

Primary Software		
Software	Description	Purpose
Endpoint Software	Windows/Mac/Linux/iOS /Android	Performs remote desktop function
BinaryDefense	Managed Detection and Response (MDR)	MDR
Devo	SaaS Security Information and Event Management (SIEM)	MDR/SIEM
AWS CloudTrail	AWS Software	Auditing events
AWS Shield	Linux	Distributed-denial-of service (DDoS) protection service
AWS Inspector	Vulnerability Management	Automated Software Vulnerability Management
AWS Route 53	Domain Name System	DNS Management
Azure Identity and Access Management (IAM)	Cloud IAM	User authentication, support business operations
Microsoft Active Directory (AD)	IAM	User account authentication and system management

## *People*

Splashtop staff is organized in the following functional areas:

- Corporate Executives: senior operations staff, and company administrative support staff, such as legal, compliance, contracting, accounting, finance, and human resources
- Operations: Staff that handles day-to-day selling of Splashtop services, including sales, support, and customer success:
  - Sales: staffing for inbound and outbound sales calls, chats, and e-mails
  - Support: staff for supporting Splashtop remote access/control services to customers via e-mails, chat, and tickets
  - Customer Success: staff to follow up with customers to ensure a positive experience with the purchasing, support, and usage of the Splashtop remote service
  - Engineering: Staff for continuous development of features and improvements to the Splashtop software and services. This team includes Windows, Macintosh, iOS, Android, Linux, and backend developers as well as a quality assurance (QA) team

## *Data*

Data as defined by Splashtop constitutes the following:

- Corporate data:
  - Product Intellectual Property
  - Engineering source code
  - Individual backups
- Customer data:
  - Customer accounts
  - Device information
  - Session logs
  - Subscription details
  - Software inventory
  - Antivirus details (Resell feature)

Product Intellectual Property and engineering source code are maintained on separate networks. The code is checked in and out with revision control. The source code is for building releases of the Splashtop software applications and the backend web console.

Customers create an account in Splashtop systems. Customers use this account to utilize and manage the Splashtop services. The customer data includes account e-mail, session logs, and system information, such as device details, software inventory, and antivirus details.

## *Processes, Policies and Procedures*

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Splashtop policies and procedures that define how services should be delivered. These are located on the Company's SharePoint site and can be accessed by Splashtop team members.

## Physical Security

The in-scope system and supporting infrastructure is hosted by AWS, GCP, and OCI. As such, AWS, GCP, and OCI are responsible for the physical security controls for the in-scope remote desktop services. Refer to the "Subservice Organizations" section below for controls managed by the subservice organizations.

## Logical Access

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

Approval processes are in place to request higher levels of data access. The department heads review and approve/decline access after reviewing the request.

Employees and approved vendor personnel sign on to the Splashtop network using an AD user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of AD. Passwords conform to defined password standards and are enforced through parameter settings in the AD. These settings are part of the configuration standards.

Employees accessing the system from outside the Splashtop network are required to use a token-based multifactor authentication (MFA) system. Employees use a Virtual Private Network (VPN) software which includes MFA. Vendor personnel are not permitted to access the system from outside the Splashtop network.

## Computer Operations - Backups

Customer data is stored on AWS system and automatically backed up. Backup restoration tests are performed daily. Backup and restoration results are reviewed upon completion. The backup retention period is two years and backup data are replicated to multiple regions. This provides failover redundancy and backups as needed of the customer data.

## Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT 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.

Splashtop monitors the capacity utilization of physical and computing infrastructure to ensure that service has a high-level of availability. Splashtop evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage
- Computing power
- Network bandwidth and latency

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

Splashtop infrastructure includes fault tolerance with cross-geographical coverage and multi-cloud servers. Additionally, Splashtop implements self-healing techniques. Splashtop monitors 24/7 for alerts with shifts for the Development and Operations (DevOps) team.

## Change Control

Splashtop maintains documented Software 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, QA 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. QA testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals.

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.

## Data Communications

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

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

Vulnerability scanning is performed by a third-party vendor on at least an annual basis in accordance with Splashtop policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Splashtop. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Splashtop system are implemented through the change management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of VPN technology. Employees are authenticated through the use of a token-based MFA system.

## **Boundaries of the System**

The scope of this report includes the Remote Desktop Services System performed in the Cupertino, California; Taipei, Taiwan; and Hangzhou, China facilities.

This report does not include the cloud hosting services provided by AWS, GCP, OCI, or the security monitoring services provided by Devo.

## Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

## Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

## Criteria Not Applicable to the System

All Common Criteria/Security and Confidentiality criterion were applicable to the Splashtop's Remote Desktop Services System.

## Subservice Organizations

This report does not include the cloud hosting services provided by AWS, GCP, OCI, or the security monitoring services provided by Devo.

### *Subservice Description of Services*

AWS provides the customer database, API servers, and relay servers for establishing remote connections. GCP and OCI provide relay servers for additional reliability. Devo services monitors logs to quickly catch any potential security concerns.

### *Complementary Subservice Organization Controls*

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.



Subservice Organization - AWS		
Category	Criteria	Control
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Key Management Service (KMS)-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		KMS-Specific - Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - GCP		
Category	Criteria	Control
Common Criteria / Security	CC6.4, CC7.2	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, biometric identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.

The following subservice organization controls should be implemented by OCI to provide additional assurance that the Trust Services Criteria described within this report are met:

<b>Subservice Organization - OCI</b>		
<b>Category</b>	<b>Criteria</b>	<b>Control</b>
Common Criteria / Security	CC6.4, CC7.2	OCI evaluates the data center and Point of Presence (PoP) site's control environment, including physical security controls and environmental safeguards, prior to the site hosting production traffic (go-live). Identified issues are evaluated and tracked through resolution.
		OCI performs an assessment of in-scope data center and PoP site's control environments, including physical security controls and environmental safeguards, in accordance with the schedule defined in the Data Center Assessment Program. Identified issues are evaluated and tracked through resolution.
		OCI reviews in-scope data center and PoP site's provider attestation reports, or internationally recognized certifications, at least annually. Identified issues are evaluated and tracked through resolution. In the event that a site does not have an attestation report, or internationally recognized certification, OCI performs an assessment annually of the site's control environment, including physical security controls and environmental safeguards.
		Physical access to data halls in the Availability Domains and PoPs is approved prior to access being granted.
		Permanent physical access to data halls in the Availability Domains and PoPs is revoked upon termination.
		Users with permanent physical access to data halls in the Availability Domains and PoPs are reviewed at least quarterly. Issues identified during the review are investigated and remediated.

The following subservice organization controls should be implemented by Devo to provide additional assurance that the Trust Services Criteria described within this report are met:

<b>Subservice Organization - Devo</b>		
<b>Category</b>	<b>Criteria</b>	<b>Control</b>
Common Criteria / Security	CC6.6, CC6.7, CC7.1, CC7.2	Devo manages the intrusion detection and notify Splashtop upon intrusion.

Splashtop management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, Splashtop performs monitoring of the subservice organization controls, including the following procedures:

- Obtaining and reviewing attestation reports
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

## COMPLEMENTARY USER ENTITY CONTROLS

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

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

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