



**REPORT ON MACSTADIUM, INC.'S HOSTED
INFRASTRUCTURE SYSTEM RELEVANT TO
SECURITY AND AVAILABILITY FOR THE
PERIOD DECEMBER 1, 2018 TO
NOVEMBER 30, 2019**

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report.....3

SECTION 2

Assertion of MacStadium, Inc. Management.....6

ATTACHMENT A

MacStadium, Inc.'s Description of the Boundaries of Its Hosted Infrastructure System.....8

ATTACHMENT B

Principal Service Commitments and System Requirements.....12

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: MacStadium, Inc. ("MacStadium")

Scope

We have examined MacStadium's accompanying assertion titled "Assertion of MacStadium, Inc. Management" (assertion) that the controls within MacStadium's Hosted Infrastructure System (system) were effective throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that MacStadium's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*).

Service Organization's Responsibilities

MacStadium 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 MacStadium's service commitments and system requirements were achieved. MacStadium has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, MacStadium is responsible for selecting, and identifying in its assertion, the applicable trust service 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 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 controls were not effective to achieve MacStadium'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 MacStadium'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.

Opinion

In our opinion, management's assertion that the controls within MacStadium's Hosted Infrastructure System were effective throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that MacStadium's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
January 17, 2020

SECTION 2

ASSERTION OF MACSTADIUM, INC. MANAGEMENT



Assertion of MacStadium, Inc. Management

We are responsible for designing, implementing, operating and maintaining effective controls within MacStadium, Inc.'s ("MacStadium") Hosted Infrastructure System (system) throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that MacStadium's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in attachment A 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 December 1, 2018 to November 30, 2019, to provide reasonable assurance that MacStadium's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). MacStadium'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 attachment B.

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 December 1, 2018 to November 30, 2019 to provide reasonable assurance that MacStadium's service commitments and system requirements were achieved based on the applicable trust services criteria.

MacStadium, Inc.

ATTACHMENT A

MACSTADIUM, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS HOSTED INFRASTRUCTURE SYSTEM

TYPE OF SERVICES PROVIDED

MacStadium, Inc. (“MacStadium” or “the Company”) is a privately held company with corporate headquarters located in Atlanta, Georgia. MacStadium provides dedicated data center infrastructure-as-a-service solutions for DevOps teams, Software-as-a-Service providers, and Enterprise organizations around the world.

MacStadium’s hosted infrastructure is primarily used by customers in the development, testing, and deployment of iOS and macOS software applications and may consist of the following technologies from vendors such as Apple, Cisco, Pure Storage, HPE, and VMware:

- Dedicated Network Routers and Switches
- Physical/Virtual Firewall Appliances
- Physical/Virtual Load Balancing Appliances
- Server/Desktop Computers
- Virtualization Software
- SAN/NAS/DAS Disk Storage
- Internet Connectivity/Transport
- IP Addressing

The boundaries of the system are the specific aspects of MacStadium’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as follows:

INFRASTRUCTURE

The Company utilizes Amazon Web Services (AWS), zColo, Equinix, and Keppel to provide the resources to host the Hosted Infrastructure System. MacStadium leverages the experience and resources of AWS, zColo, Equinix, and Keppel to enable MacStadium to quickly and securely scale as necessary to meet current and future demand. However, MacStadium is responsible for designing and configuring the Hosted Infrastructure System architecture within the hosting provider’s environments to ensure the availability, security, and resiliency requirements are met. Specifically, service is provided to Customers using IT equipment that is hosted in the following MacStadium private cage data center facilities:

Hosted Locations	
Provider	Location
AWS	<ul style="list-style-type: none">• US-East-1• US-West-2
Equinix	<ul style="list-style-type: none">• Sunnyvale, California• Frankfurt, Germany
zColo	<ul style="list-style-type: none">• Atlanta, Georgia• Las Vegas, Nevada

Hosted Locations	
Provider	Location
Keppel	<ul style="list-style-type: none"> • Dublin, Ireland

In order to deliver the services to customers, MacStadium has deployed the following hardware from various technology vendors in its internal management network:

- Network Routers
- Network Ethernet Switches
- FiberChannel Storage Switches
- Physical/Virtual Firewall Appliances
- Physical/Virtual Load Balancing Appliances
- Blade Servers
- SAN/NAS/DAS Disk Storage
- Internet Connectivity/Transport
- IP Addressing

SOFTWARE

The Company utilizes the following application programs and IT system software in support of the MacStadium infrastructure.

- MacStadium Internal Admin Portal
- MacStadium Customer Portal
- Application & Infrastructure Monitoring Applications
- Virtualization Management Software
- Backup and Replication Software
- Security Incident Event Management (SIEM) and Logging Systems
- Vulnerability & Patch Management Systems
- Advanced Anti-Virus & Anti-Malware Endpoint Protection
- Intrusion Detection and Prevention Systems

PEOPLE

Services are provided by MacStadium Operations, Security & Compliance, Customer Support, Sales, Account Management, Software Development, Product Development, Engineering, and Executive Management teams.

All MacStadium teams are recruited and managed using MacStadium policies and procedures which are described in the following sections.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the Hosted Infrastructure System. MacStadium has the following security procedures and policies in place, which are owned by the Chief Information Security Officer:

- Security awareness
- Risk management
- Identity management
- Logical and physical access control
- Enterprise change management
- Incident / problem management
- Disaster recovery
- Backup and offsite storage
- Threat and vulnerability management
- Internal and external auditing
- Full software development lifecycle

Policies are reviewed at least annually and may be reviewed more frequently if necessary. Members of the Security Executive Committee are authorized to perform reviews of policies with final approval for changes from the Chief Information Security Officer in conjunction with other senior management. Approvals are documented electronically as they occur. Any changes to the policies are then communicated to employees electronically and are posted on an internal SharePoint site accessible to employees.

To mitigate any potential for loss or exploitation of sensitive data, MacStadium maintains a data classification policy to determine whether the appropriate controls are in place for data of higher sensitivity. This policy classifies data into categories and specifies protection accordingly.

DATA

Data refers to transaction streams, files, data stores, tables, and output used or processed by MacStadium. MacStadium does not electronically access data within the Customer's dedicated infrastructure environment. All Customer data is managed, transmitted, and stored within their environment at their sole discretion. Customer data is handled in accordance with relevant data protection and other regulations, with any specific requirements formally established in customer contracts and service orders.

The Company has deployed secure methods and protocols for transmission of confidential and/or sensitive information over public networks.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the MacStadium Hosted Infrastructure System. Commitments are communicated in standardized contracts and service level agreements.

System requirements are specifications regarding how the MacStadium Hosted Infrastructure System should function to meet MacStadium’s principal commitments to user entities. System requirements are specified in MacStadium’s policies and procedures, which are available to all employees.

MacStadium’s principal service commitments and system requirements related to the MacStadium Hosted Infrastructure System include the following:

Trust Services Category	Service Commitments	System Requirements
<p>Security</p>	<ul style="list-style-type: none"> • MacStadium will maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of the Services. 	<ul style="list-style-type: none"> • Logical access standards • Employee provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection standards • Risk and vulnerability management standards • Incident handling standards • Change management standards • Vendor management
<p>Availability</p>	<ul style="list-style-type: none"> • In each twelve (12) month period, MacStadium will have at least 99.99% availability for the Services outside of emergency maintenance and Scheduled Maintenance (if applicable). • Scheduled Maintenance shall not cause a loss of availability of the Services unless necessary to complete the Scheduled Maintenance. MacStadium shall use reasonable efforts to ensure any loss of availability of Services arising from Scheduled Maintenance is limited to the shortest period of time practical. 	<ul style="list-style-type: none"> • System monitoring • Backup and recovery standards • BC/DR Plans and Testing