REPORT ON MACSTADIUM, INC.'S HOSTED INFRASTRUCTURE SYSTEM RELEVANT TO SECURITY AND AVAILABILITY FOR THE PERIOD DECEMBER 1, 2019 TO NOVEMBER 30, 2020

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

COALFIRE CONTROLS

TABLE OF CONTENTS

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, 2019 to November 30, 2020, 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, 2019 to November 30, 2020, 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 11, 2021

SECTION 2

ASSERTION OF MACSTADIUM, INC. MANAGEMENT

Assertion of MacStadium, Inc. (“MacStadium”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within MacStadium’s Hosted Infrastructure System (system) throughout the period December 1, 2019 to November 30, 2020, 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, 2019 to November 30, 2020, 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*). 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, 2019 to November 30, 2020 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, GA, USA. MacStadium provides dedicated data center infrastructure-as-a-service (IaaS) solutions for Development and Operations (DevOps) teams, software-as-a-service (SaaS) providers, and enterprise organizations around the world.

MacStadium’s hosted infrastructure is primarily used by customers for the development, testing, and deployment of iOS and macOS software applications and may consist of the following technologies from various vendors:

- Dedicated network routers and switches
- Physical or virtual firewall appliances
- Physical or virtual load balancing appliances
- Server and desktop computers
- Virtualization software
- Storage area network (SAN), network-attached storage (NAS), and direct-attached storage (DAS)
- Internet connectivity and transport
- Internet Protocol (IP) addressing

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

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 described in the subsections below.

Infrastructure

The Company utilizes third parties to provide the resources to host MacStadium’s Hosted Infrastructure System. MacStadium leverages the experience and resources of the hosting providers to enable MacStadium to scale quickly and securely 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 that availability, security, and resiliency requirements are met. Specifically, service is provided to customers using information technology (IT) equipment that is hosted in MacStadium private cage data center facilities.

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
- Fiber channel storage switches
- Physical and virtual firewall appliances
- Physical and virtual load balancing appliances

- Blade servers
- SAN, NAS, and DAS
- Internet connectivity and 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 and infrastructure monitoring applications
- Virtualization Management software
- Backup and replication software
- Security information and event Management (SIEM) and logging systems
- Vulnerability and patch Management systems
- Advanced antivirus (AV) and anti-malware endpoint protection
- Intrusion detection and prevention systems

People

Services are provided by MacStadium's Operations, Security and 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 section.

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 (CISO):

- Security awareness
- Risk Management
- Identity Management
- Logical and physical access control
- Enterprise change Management
- Incident and problem Management
- Disaster recovery
- Backup and offsite storage
- Threat and vulnerability Management
- Internal and external auditing

- Full software development life cycle

Policies are reviewed at least annually and may be reviewed more frequently if necessary. Members of the Security Executive Committee are authorized to perform policy reviews with final approval for changes from the CISO 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 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 sensitivities. 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.

SUBSERVICE ORGANIZATIONS

MacStadium uses subservice organizations for data center colocation services. MacStadium's controls related to the Hosted Infrastructure System cover only a portion of the overall internal control for each user entity of the Hosted Infrastructure System. The description does not extend to the services provided by the subservice organizations that provide colocation services for IT infrastructure.

Although the subservice organizations have been carved out for the purposes of this report, controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Management of MacStadium receives and reviews the subservice organizations' SOC 2 reports annually. In addition, through its operational activities, MacStadium Management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreements, stay abreast of changes planned at the hosting facilities, and relay any issues or concerns to management of the subservice organizations.

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 MacStadium's Hosted Infrastructure System. Commitments are communicated in standardized contracts and service-level agreements.

System requirements are specifications regarding how MacStadium's 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 MacStadium's Hosted Infrastructure System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• MacStadium will maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of the services. • MacStadium will notify customer of any data breach as soon as practicable, and without undue delay, after becoming aware of the breach.	• 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
Availability	• MacStadium will maintain at least 99.9% uptime in a calendar month for the services outside of emergency maintenance and scheduled maintenance. • MacStadium will use reasonable effort to ensure that any loss of availability of services arising from scheduled maintenance is limited to the shortest period of time practical. • MacStadium commits to system availability as specified under customer contracts.	• System monitoring • Backup and recovery standards • Business continuity/disaster recovery (BC/DR) plans and testing