MacStadium

Technical and Organizational Measures (TOMs) – Security Services

The technical and organizational measures ("TOMs") apply to all standard service offerings provided by MacStadium, Inc. ("MacStadium") Security except where Client is responsible for security and privacy TOMs. MacStadium may change the TOMs from time to time to adapt to the evolving security landscape and where required will notify customers of these changes. Evidence of the measures implemented and maintained by MacStadium Security may be presented in the form of up-to-date attestations, reports or extracts from independent bodies upon request from the Client.

Document Management

MacStadium will validate that necessary documentation is in place between MacStadium and the Client where MacStadium processes any information relating to a person or entity that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person or entity ("Personal Data") covered by the General Data Protection Regulation ("GDPR"). In case of a change to the defined scope, any change to the processing of Personal Data will be reviewed to determine any impact on required TOMs and other contract exhibits.

MacStadium will create and maintain the following security and privacy documentation as well as store them in a central repository with restricted access control:

a. Data Privacy Agreement ("DPA")
b. TOMs
c. Non-disclosure Agreement ("NDA") or Confidentiality Information or similar (as required)
d. Sub-processor Agreement (as required)
   Note: MacStadium's Sub-Processors are listed here: https://www.macstadium.com/sub-processors

Security Incidents

MacStadium will maintain an incident response plan and follow documented incident response policies in compliance with our published security procedures and ISO certifications. MacStadium shall send applicable data breach notifications to the legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data ("Data Controller") without undue delay where a breach is known or reasonably suspected to affect Client Personal Data.

Risk Management

MacStadium will assess risks related to processing of Personal Data and create an action plan to mitigate identified risks.

Security Policies

MacStadium will maintain and follow IT security policies and best practices that are integral to

MacStadium's business and mandatory for all MacStadium employees, including supplemental personnel. IT security policies will be reviewed periodically and MacStadium will amend such policies as reasonably necessary to maintain protection of services and content processed therein.

MacStadium will maintain an inventory of Personal Data reflecting the instructions set out in the DPA, including disposal instructions upon contract termination, as applicable. Computing environments with resources containing Personal Data will be logged and monitored.

MacStadium employees will complete security and privacy education annually and certify each year that they will comply with MacStadium's ethical business conduct, confidentiality, and security policies, as set forth in MacStadium's internal policies.

Physical Security

MacStadium will implement physical security of all MacStadium facilities, including third party data centers, and take necessary precautions against environmental threats and power disruptions for Clients. Access to its data centers and controlled areas within the data center will be limited by job role and subject to authorized approval. MacStadium will maintain visitor management systems implemented for all visitors/guests.

User Access Management

MacStadium will maintain proper controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications containing Personal Data. Only employees with clear business needs access to Personal Data located on servers, within applications, databases and/or have the ability to download data within MacStadium's network. All access requests will be approved by management based on individual role-based access and reviewed on a regular basis for continued business need. All systems must meet corporate IT Security Standards and employ security configurations and security hygiene practices to protect against unauthorized access to operating system resources ("OSR").

System and Network Security

MacStadium will employ encrypted and authenticated remote connectivity to MacStadium computing environments and Client system unless otherwise directed by the Client.

For Private Cloud User Clients

MacStadium will implement TOMs to support the security of its network and confirm the availability of computing environments and access to Client Personal Data. Network security measures such as firewalls, network segmentation, and two-factor authentication are used in general for access to the critical MacStadium target systems.

Controls and Validation

MacStadium Security will maintain policies and procedures designed to manage risks associated with the application of changes to the changes to the MacStadium systems.

Workstation Protection

MacStadium will implement protections on end-user devices and monitor those devices to be in

compliance with the security standard requiring hard drive passwords, screen savers, antivirus software, firewall software, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are consistently applied to detect and remediate workstation compliance deviations.

MacStadium will securely sanitize physical media intended for reuse prior to such reuse and refer to the MacStadium Data Destruction and Sanitization Policy ("DDSP") for any applicable destruction procedures.

Threat and Vulnerability Management

MacStadium will maintain industry standard measures to identify, manage, mitigate and/or remediate vulnerabilities within the MacStadium computing environments. Certain Security measures include:

- Patch management of operating systems, firmware, productivity applications, and utilities used in all MacStadium systems, equipment, and facilities
- Anti-virus / anti-malware
- Threat notification advisories
- Vulnerability scanning (all internal systems) and periodic penetration testing (public internet facing systems) within remediation of identified vulnerabilities