System Description of the MURAL System

SOC 3

Relevant to Security and Confidentiality

APRIL 1, 2019

TO

MARCH 31, 2020

TABLE OF CONTENTS

I. Independent Service Auditor's Report

MOSSADAMS

MURAL
2000 Broadway Street #1108
San Francisco, CA 94115

To the Management of MURAL:

Scope

We have examined MURAL's accompanying assertion in Section II titled "Assertion of MURAL Management" (assertion) that the controls within its MURAL System (system) were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that MURAL'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* (AICPA, *Trust Services Criteria*).

MURAL uses subservice organization Microsoft Azure to maintain the MURAL website production environment. Our examination did not extend to the services provided by the subservice organization.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of MURAL's controls are suitably designed and operating effectively, along with related controls at MURAL. We have not evaluated the suitability of design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

MURAL 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 MURAL's service commitments and system requirements were achieved. MURAL has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, MURAL 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 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 (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 the description is presented in accordance with the description 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 its MURAL System were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that MURAL's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

San Francisco, California
June 16, 2020

II. ASSERTION OF MURAL'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within its MURAL System (system) throughout the period April 1, 2019 to March 31, 2020 to provide reasonable assurance that MURAL's service commitments and system requirements relevant to Security and Confidentiality were achieved. Our description of the boundaries of the system is presented in Section III entitled "MURAL's Description of the Boundaries of Its MURAL System" 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 April 1, 2019 to March 31, 2020, to provide reasonable assurance that MURAL'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* (AICPA, *Trust Services Criteria*). MURAL'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 Section III entitled "MURAL's Description of the Boundaries of Its MURAL System".

MURAL uses subservice organization Microsoft Azure to maintain the MURAL website production environment. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at MURAL, to achieve MURAL's service commitments and system requirements based on the applicable trust services criteria. The description presents MURAL's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of MURAL'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 April 1, 2019 to March 31, 2020, to provide reasonable assurance that MURAL's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. MURAL'S DESCRIPTION OF THE BOUNDARIES OF ITS MURAL SYSTEM

A. SYSTEM OVERVIEW

1. SERVICES PROVIDED

Founded in 2011, Tactivos Inc., doing business as MURAL, is incorporated in Delaware, United States, with offices in San Francisco, California and development operations in Buenos Aires, Argentina.

MURAL system is a digital workspace that features "murals", digital whiteboards which are accessible online. A "mural" is a large, shared canvas to map all kinds of content to share inspiration, discover new insights, brainstorm, organize ideas, and define solutions. Companies use MURAL's software to embrace distributed creative problem solving. The collaborative workspace enables teams to communicate in real-time and asynchronously in various ways: via chat, inline comments, following teammates, voting, and more.

MURAL offers customers its enterprise-class software in a simple and secure on-demand SaaS (Software-as-a-Service) platform, substantially reducing the amount of risk and capital outlay typically associated with Enterprise software implementations.

2. INFRASTRUCTURE

MURAL is mainly hosted on Microsoft Azure East US (Virginia) data centers in the United States. Every service component on the system is designed to leverage cloud provider's fail-over and high-availability capabilities.

MURAL's production systems are hosted within the Microsoft Azure. The platform has implemented network and operation security controls that are evaluated as part of the vendor management process.

The MURAL application uses a distributed micro-services architecture. Micro-services are small, independent processes that communicate with each other to form complex applications which utilize language-agnostic Application Program Interfaces (APIs). These services are small building blocks, highly decoupled, and focused on doing a small task, facilitating a modular approach to system-building.

Micro-services are interconnected on an isolated cloud virtual network that provides linking between them without the need for advanced firewall configurations.

MURAL development, staging, and quality assurance (QA) environments are separated from the production environment. Customer data only resides in the production environment, and transferring, scrambling, or utilizing customer's information outside production environments is forbidden by company's policies and procedures.

MURAL encrypts all customer data both at rest (using hard disk encryption built in to cloud provider's infrastructure) and in transit (using Transport Layer Security (TLS) certificates and public/private keys).

In addition to secure coding practices, a vulnerability self-assessment, including penetration testing, is performed annually by the Operations team with the help of third party vendors in order to identify any application and network vulnerabilities. Periodic vulnerability assessments of production site perimeters, including penetration testing, are conducted by a third party. Penetration testing is completed on an annual basis. Results are reviewed by management and tracked through resolution.

Multiple monitoring systems are in place to monitor overall site performance, as well as monitor the individual infrastructure components. Production systems are monitored for availability, performance, and security issues. Documented procedures exist for the escalation of systems availability issues, and potential security breaches which cannot be resolved by MURAL's Support team. Production services are monitored for system or process failures, availability, downtime, growth/capacity issues, and throughput. Alerts are designed to send out instant notification to key personnel in the event of a failure or reaching of a critical threshold. These operational incidents, including ones identified during the system monitoring process, are tracked through to resolution in a ticketing system.

MURAL has built in a number of redundant critical systems. In order to ensure 24x7 availability and to meet service level agreement (SLA) uptime requirements for customers of 99.9% (not including Microsoft Azure schedule maintenance windows) MURAL has built in a number of duplications of critical system components (redundancy) into the production environment.

The purpose of introducing this level of redundancy is to increase system reliability, enable fault tolerance, and minimize single points of failure.

MURAL has established procedures for incident response documented in the Incident Response Policy that also contains the escalation and communication policies. Any detected security incident is processed using MURAL's Incident Response Policy.

Incidents reported by internal or external users are tracked within a ticketing system. All issues are assigned a severity level and assigned to appropriate personnel to resolve. Any system outages are documented on an external site (https://status.mural.co) that provides detailed information on System Outage Reports, including the date and time of the outage, location/source, duration, error or reason, and follow-up action items.

3. **SOFTWARE**

MURAL system features include:

- *Teams* – A comprehensive way for organizations to create workgroups and manage their permissions within MURAL.
- *Rooms* – Users can organize their murals, like using operating system folders. Users can invite people directly to a room. Room members get access to all the murals inside that room.
- *Murals* – A large, shared canvas to map all kinds of content to share inspiration, discover new insights, brainstorm, organize ideas, and define solutions.
- *Voting* – Designed to give users the ability to quickly form a hierarchy of ideas and improve idea synthesis.

- *Search* – A secured indexing system that allows users to search for content (murals, rooms, or templates) to which they have access.
- *Reporting and Dashboards* – Used for assessment data, activity, and usage.
- *Integration Features* – This includes Security Assertion Markup Language (SAML) 2.0 and OAuth (Open Authorization Protocol) based Single Sign On and RESTful APIs.

4. PEOPLE

ORGANIZATION STRUCTURE

MURAL's leadership team consists of a Chief Executive Officer (CEO), Head of Customer Success & Education, a Chief Technology Officer (CTO), and the Head of Sales. Each leadership team reports directly to the CEO.

Each of the above members of the management team has a distinct, separate responsibility within the organization. Roles and responsibilities have been segregated to the extent possible. MURAL has an up-to-date functional organization chart which defines the organizational structure, reporting lines, authorities, and responsibilities.

Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to the Chief Technology Officer (CTO).

Job descriptions for the employees responsible for the design, development, and operation of the MURAL system are available and include employee qualifications such as experience and education and daily job responsibilities.

MURAL has a staff of approximately 120 employees organized in the following organizations:

- Customer Success & Education
- Product Development
- Compliance, Technology, and Research & Development (R&D)
- Operations, Finance & Human Resources
- Sales

Approximately 50% of employees belong to the Compliance, Technology, and R&D Organization. MURAL does not utilize any external personnel designing, developing, implementing, operating, maintaining, or monitoring controls.

RECRUITING AND TALENT ACQUISITION

Jobs openings are posted on the MURAL job board site, as well as on social networks, and job sites such as LinkedIn, Angel.co and StackOverflow careers. MURAL conducts interviews and background checks on employees.

As part of the recruiting process to ensure the potential candidates are qualified for the position, interview notes and technical assignment results are maintained. New personnel hired in the United States and responsible for the design, development, and operation of the MURAL system are offered employment subject to background checks.

ORIENTATION AND PERSONNEL MANAGEMENT

All employees responsible for the design, development, and operation of the MURAL system are required to review policies and procedures as a part of the new hire on-boarding process. These policies are also available on the MURAL compliance documentation repository. As part of new hire orientation, MURAL employees review and acknowledge the Employee Handbook and Information Security Policies.

Workplace conduct standards are established in the Code of Conduct policy, which is available to the company employees. Employees responsible for the design, development, and operation of the MURAL system are responsible for reviewing and acknowledging the policy during the hiring process and annually thereafter. The Code of Conduct policy specifies the disciplinary actions for enforcing procedures.

Non-Disclosure Agreements (NDAs) are in place between MURAL and its employees responsible for the design, development, and operation of the MURAL system during the on-boarding and annually thereafter.

MURAL provides documentation for employees to ensure that the personnel have the information necessary to carry out the responsibilities as they relate to the design, development, implementing, operating, maintaining, and monitoring controls.

MURAL employees are provided information on how to report security failures, incidents, concerns, and other complaints through the Employee Welcome On-Boarding document.

MURAL has an established performance review program for the engineering personnel, and reviews are completed annually for these employees.

5. **DATA**

MURAL does not request, store, or transfer customer personably identifiable information (PII) or electronic personal health information (ePHI) to or in its database. MURAL has a Terms of Use and Privacy Policy that are reviewed periodically. The Terms of Use and Privacy Policy can be found on MURAL's website. MURAL has a signed NDA in place with third-party providers prior to using their services. The CEO or CTO updates the NDA, Privacy Policy, and Terms of Use whenever changes to commitments and requirements are needed.

Logical access controls are in place and data is logically partitioned such that employee, customer, and provider accounts cannot see the data for any other user. System logs are available for detection of unauthorized access.

The MURAL site renders pages and delivers its data using JavaScript Object Notation (JSON) via secure Hypertext Transfer Protocol (HTTP) connections using Transport Layer Security (TLS) v1.2 to encrypt data between the application and the servers. MURAL uses a grade A transport level security protocol to encrypt data between the application and the servers.

MURAL logs and validates incoming and outgoing data from its Representational State Protocol (REST) API. The REST API returns error messages in a requested format.

Sensitive data, such as external user passwords for the customers signing up directly with MURAL (without Single Sign On) are stored hashed and salted at the field level within the database. For customers with Single Sign On or Google Authentication enabled, MURAL does not have access to or stores their passwords.

Customer data removal policies and procedures exist to provide guidance for MURAL employees. Customer data is removed when requested by authorized personnel.

Data is secured using backup encryption processes. Backups are encrypted, with the data encryption key not stored with the data. Backups are stored on the same cloud provider with redundancy and encrypted using 256-bit AES encryption. The encryption is accomplished using the built-in server side encryption mechanisms on Azure along with its automated key rotation features. Only authorized individuals can access customer data.

6. PROCESSES AND PROCEDURES

MURAL has a formal System Development Lifecycle (SDLC) methodology addressing security and confidentiality commitments that governs the design, acquisition, implementation, configuration, testing, modification, and maintenance of system components. MURAL has a formal change management procedure, all changes to production, including emergency changes, go through a formal change control process that requires testing and approval before migration to the production environment, in accordance with security and confidentiality commitments. MURAL follows a weekly sprint product development lifecycle. MURAL change management policies and procedures describe the main procedures and activities required to carry out development duties. Software deployments happen as they are approved by the Development team and after code is reviewed, and all the security, unit, smoke, and manual testing is completed in a test environment. Code review is completed for software changes. Test environments are automatically created as change requests (pull request) are opened on the source code versioning tool. These are automatically disposed of once the change request is integrated into the mainline. Segregation of duties exists between developers generating the code and developers releasing changes into the production environment, and it is enforced through a system-level control.

Customer data removal policies and procedures exist to provide guidance for MURAL employees.

Policy changes and approval are managed with the same techniques described on the Change Management Policy. By using this techniques MURAL obtains the following benefits:

- Changes and reviews are automatically tracked.
- Modifications are clearly spelled out. Each modification has a date, title, and description.

- The author of each modification is identified.

- There is a history of the document since it was first created.

- Only internal users can have access to the documents.

- Only defined roles have the access to make changes in the documents. Any other user can suggest changes, but they must be approved by the manager.

- Segregation of duties is maintained.

The Information Security Policy is communicated to all employees as part of new hire orientation and employees as part of their ongoing annual review, and is available for inspection at any time through the MURAL compliance documents repository. Information Security Policies have been developed to provide a framework to ensure the security and confidentiality MURAL information systems.

Security policies are reviewed annually and updated to remain consistent with system commitments and requirements.

Product documentation for customers listing the description of the system and its boundaries are available on the support portal and within the User Agreements. For Enterprise tier customers and/or special exceptions, customer responsibilities are specified through the contracts between the customers and the company. MURAL publishes the Privacy Policy and Terms of Use for customers to understand MURAL's commitments to security on their website. Changes to MURAL's confidentiality commitments are communicated to internal and external users via an email communication as defined in the Information Security Policy. Customer data is retained as documented in MURAL's Privacy Policy. Customer data is disposed upon customer request.

MURAL performs four-hour snapshots and daily, weekly, and monthly encrypted backups. MURAL uses its monitoring systems to analyze and identify trends that may have an impact on MURAL's ability to achieve its uptime services levels. Production systems are monitored for availability and performance issues to meet MURAL's service level objective of 99.9% uptime. Alerts are designed to send out instant notification to key personnel in the event of a failure or reaching of a critical risk threshold. These operational incidents are tracked in a ticketing system through to resolution.

B. PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

MURAL's service commitments are documented in its contracts with customers. Among other items, they include:

- Protecting customer data by maintaining a security program designed to ensure the security and integrity of customer data and prevent unauthorized access to it.

- Acting in accordance with MURAL's documented Privacy Policy for end users of the system.

All customers must enter into an agreement with MURAL in order to access the subscription services.

MURAL service system requirements are documented and communicated to employees through internal policies, standards, and procedures. These materials are available to all team members and they agree to abide by them at hire. The requirements include:

- System access is implemented according to need-to-know, least privilege, and separation of duties.
- System changes are managed according to change control procedures.
- Confidential data is encrypted in transit and at rest.
- System components are monitored for security performance.
- Risks are managed, and acknowledged by executive leadership.

C. COMPLEMENTARY USER ENTITY CONTROLS

MURAL's MURAL System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its MURAL System. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at MURAL. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls

1	Understanding and complying with their contractual obligations to MURAL.
2	Alerting MURAL about any regulatory changes within their industry that might affect their services.
3	Defining a unique user ID and password, and standard identity management settings such as: session time out, password complexity, password length, disable account after a number of failed logon attempts, if Single Sign On or Google Authentication are enabled.
4	Treating MURAL account sign-in name and password information as secure and private and in accordance with industry best practices, if Single Sign On or Google Authentication are not enabled.
5	Accounting for and informing MURAL of any changes to contact names, phone numbers, email addresses, etc.
6	Ensuring that personnel are properly trained in the use of the MURAL service.
7	Ensuring that users are trained on security awareness.
8	Performing all account administration activities, including adding and removing users with access to their system.