SMITH+HOWARD

Formerly GEELS | NORTON

Tactivos, Inc. d/b/a Mural

Visual Collaboration Platform

System and Organization Controls (SOC) 3 Report

Report on Mural's Description of its Visual Collaboration Platform System and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security and Confidentiality

Throughout the Period April 1, 2025 to March 31, 2026

Table of Contents

I. INDEPENDENT SERVICE AUDITOR'S REPORT 3

II. ASSERTION OF MURAL MANAGEMENT 6

III. MURAL'S DESCRIPTION OF ITS VISUAL COLLABORATION PLATFORM SYSTEM 8

IV. PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 14

I. Independent Service Auditor's Report

SMITH+HOWARD PC

Independent Service Auditor's Report

To the Management of Tactivos, Inc. d/b/a Mural

Scope

We have examined Tactivos, Inc. d/b/a Mural's (the "Service Organization" or "Mural") accompanying assertion, "Assertion of Mural Management" and the controls over the Visual Collaboration Platform system were effective throughout the period April 1, 2025 to March 31, 2026, 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Mural uses key third party service providers (subservice organizations) that support certain aspects of the Visual Collaboration Platform system. Management has determined that the carve-out method could be used in the system description. As such, the controls at these subservice organizations were not included in the scope of this examination, and our opinion does not extend to those controls.

Mural has indicated that certain 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. 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

Mural's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Mural's service commitments and system requirements were achieved. Mural management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the system and describing the boundaries of the system
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that the controls within the system were effective throughout the period to provide reasonable assurance that Mural's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with the 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 controls were not effective to achieve Mural'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 Mural'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 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 or 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

Mural's controls over the Visual Collaboration Platform system were effective throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that Mural's service commitments and system requirements were achieved based on the applicable trust services criteria.

Smith & Howard PC
Atlanta, Georgia
May 5, 2026

II. Assertion of Mural Management

Assertion of Mural Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Tactivos, Inc. d/b/a Mural (the "Service Organization" or "Mural") Visual Collaboration Platform system throughout the period April 1, 2025 to March 31, 2026 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 and identifies the aspects of the system covered by our assertion.

Mural uses key third party service providers (subservice organizations) that support certain aspects of the Visual Collaboration Platform system. We have determined that the carve-out method could be used in the system description. As such, the controls at these subservice organizations were not included in the scope of this examination, and our opinion does not extend to those controls. Mural has indicated that certain 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.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2025 to March 31, 2026, 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 4 of this report.

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, 2025 to March 31, 2026 to provide reasonable assurance that Mural's service commitments and system requirements were achieved based on the applicable trust services criteria.

Mural Management

III. Mural's Description of its Visual Collaboration Platform System

Overview of Operations and the System

Company Background

Founded in 2011, Mural is a Delaware-incorporated company headquartered in San Francisco, California. The company operates as a software-as-a-service (SaaS) provider and delivers its platform to customers globally over the internet. Mural maintains development operations in Argentina and supports its business through a globally distributed workforce.

Mural provides a cloud-based visual collaboration platform that is accessed by customers through supported web browsers and integrations. As the SaaS provider, Mural is responsible for the development, operation, maintenance, and security of the platform, while customers consume the service without deploying or managing underlying infrastructure.

Services Provided

The Visual Collaboration Platform ("the platform") is a cloud-based solution that enables customers to create, edit, and share interactive digital workspaces, commonly referred to as murals. These workspaces function as shared virtual whiteboards that support activities such as brainstorming, ideation, workshop facilitation, planning, retrospectives, and collaborative decision-making.

The platform supports both real-time and asynchronous collaboration and is designed for distributed, remote, hybrid, and in-person teams. Core functionality includes the creation and modification of visual elements such as text, shapes, sticky notes, and diagrams, along with features for commenting, in-canvas chat, idea voting, collaborator presence, and the use of pre-built or custom templates to structure collaboration activities.

Mural also incorporates AI-driven capabilities to enhance productivity and streamline collaboration workflows, including:

- AI-assisted idea generation to help teams quickly brainstorm and expand on concepts
- Automated summarization of workshop content, discussions, and sticky notes
- Intelligent clustering and mind map categorization of ideas to identify themes and patterns

The platform is delivered as an on-demand SaaS solution. The underlying application and supporting infrastructure are hosted and managed by Mural. Customers access the platform through authenticated user accounts via supported web browsers and integrations and are not required to deploy or manage on-premises hardware or software. Mural manages platform updates and enhancements as part of normal operations.

Infrastructure

The Platform is hosted within a Microsoft Azure cloud environment. The platform is deployed across separate Microsoft Azure cloud accounts located in the United States, Europe, and Australia to support regional data handling requirements and geographic distribution of the service. Mural also hosts customer data to support the operation of the platform in MongoDB databases. Internal access to the Visual Collaboration Platform is managed through **a** centralized identity provider responsible for authenticating users and federating authentication to downstream services.

The following table provides a high-level description of the infrastructure services used to support the platform:

Component	Purpose
AWS Route 53	AWS Route 53 is a managed domain name system service used to route internet traffic to application resources.
Azure Web Application Firewall (WAF)	Azure WAF provides protection for internet-facing application endpoints by filtering and monitoring web traffic.
Azure Network Security Groups (NSGs)	Azure NSGs are used to define and enforce network access controls within the cloud environment.
Azure Virtual Network (VNet)	Azure VNet provides a logically isolated network environment for cloud resources.
Azure NAT Gateway	Azure NAT Gateway enables controlled outbound internet connectivity for cloud resources.
Azure Application Gateway	Azure Application Gateway manages and routes web traffic to backend application services.
Azure Load Balancer	Azure Load Balancer distributes network traffic across backend resources to support availability and performance.
Azure Kubernetes Service (AKS)	Azure AKS s a managed container orchestration service used to host and scale application workloads.
Azure Virtual Machines (VMs)	Azure VMs provide virtualized compute resources to support platform operations.
MongoDB Atlas	MongoDB Atlas is a managed cloud database service used to support application data storage needs.
Azure Blob Storage	Azure Blob Storage is a cloud object storage service used to support platform operations.
Azure Cache for Redis	Azure Cache for Redis is an in-memory caching service used to support performance and efficiency.
Azure Key Vault	Azure Key Vault is a managed service used to store and manage cryptographic keys and secrets.
Azure Event Hubs	Azure Event Hubs is a managed, cloud-based event streaming service used to ingest and process high volumes of real-time data from distributed sources and perform streaming services for the platform.

Software

Mural uses a combination of software tools to support the secure development, operation, and reliability of the application. These tools support source code management, identity and access administration, monitoring and alerting, incident response, collaboration, documentation, vulnerability management, security awareness, and the responsible use of AI-powered capabilities. Collectively, they enable Mural to develop, monitor, and operate the platform efficiently while supporting its overall security and operational objectives.

People

Mural's organizational structure is designed to support effective governance, accountability, and segregation of duties across the organization. The leadership team consists of executive and senior management roles. Each member of the management team has distinct and separate responsibilities within the organization, and roles and responsibilities are segregated to the extent practicable.

Mural maintains an up-to-date functional organizational chart that defines reporting lines, authorities, and responsibilities. Job descriptions are documented for employees and include required qualifications, such as experience and education, as well as defined job responsibilities. Responsibility and accountability for the design, development, implementation, operation, maintenance, monitoring, and approval of system controls are assigned to the Chief Information Security Officer (CISO).

Mural personnel are organized across three primary functional areas, Development (R&D), Sales and Marketing (S&M), and General and Administrative (G&A). Mural's system controls are operated and monitored by internal personnel.

Functional Area	Responsibilities
R&D	The R&D function, which includes Engineering and Product, is responsible for designing, developing, testing, and maintaining the Mural platform. This function executes the software development lifecycle, implements approved system changes, remediates technical issues, and ensures that product functionality aligns with business requirements and security standards.
S&M	The S&M function, which includes Customer Experience, Revenue, and Marketing, is responsible for customer acquisition, account management, and external communications related to Mural's services. This function manages customer relationships and contractual engagements and coordinates with internal teams to ensure that customer communications and commitments align with approved policies and service capabilities.
G&A	The G&A function, which includes People, Finance and Legal, Executive, Security, Compliance, and IT, provides governance, oversight, and operational support across the

Functional Area	Responsibilities
	organization. This function is responsible for establishing organizational policies, managing enterprise risk, supporting compliance activities, and overseeing the effective operation of internal controls.

Policies and Procedures

Mural maintains the following documented policies and procedures to support the internal control environment:

- Acceptable Use of Visual Collaboration Platform systems & Assets Policy
- Account Management & Access Control Policy
- Artificial Intelligence Policy
- Asset Management Policy
- Audit Policy
- Backup Policy
- Business Continuity and Disaster Recovery Policy
- Change Management Policy
- Customer Data Retention Policy
- Data Classification Policy
- Data Container Security Policy
- Data Loss Prevention Policy
- Encryption Policy
- Firewall Management Policy
- Impersonation Policy (Internal)
- Individual Offboarding Policy
- Individual Onboarding Policy
- Information File Management Policy
- Information Security Policy
- Information Security Risk Management Policy
- Media Sanitization and Disposal Policy
- Monitoring and Logging Policy
- Mural Third Party Vendor Management Policy
- Network Security Policy
- Open Source Policy
- Patch Management Policy
- Performance Review Policy
- Public Information Security Policy
- Quality Policy
- Security Incident Management Policy
- Security Review Policy
- Third Party Vendor Management Policy
- Training & Development Policy
- Vulnerability Management Policy
- Workplace Visitor Polic

Data

Data stored and processed by the Mural platform consists of customer-generated content, including visual collaboration artifacts such as murals, objects, templates, and related workspace configuration data. The platform intentionally limits the data collected on customers and only stores personal information for authentication purposes and account management, which includes names and email addresses. Other personal information is not intended to be stored within the platform.

Customer data and backups of data are stored encrypted. Customers are able to delete their own account data or request for their accounts to be deleted from the Mural team.

Azure OpenAI is the sole AI service used to process customer data. The service is configured that customer data is not used to train OpenAI models, and customer data is not retained by the service beyond transient processing.

Data is classified by risk and controls are applied based on the classification. Data retention and data destruction policies and procedures are in place and employees are trained on the proper use and safeguards of data.

IV. Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Mural designs its processes and procedures to meet objectives for its Visual Collaboration Platform system. Those objectives are based on the service commitments that Mural makes to user entities and the system requirements that Mural has established for their services.

Security and confidentiality commitments are standardized and include implementing commercially reasonable technical, administrative, and organizational measures to protect customer data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. Additional commitments include, but are not limited to the following:

- Restricting access to system components and data to system users who require access to fulfill their job role and responsibilities
- Implementing encryption technologies to protect data from unauthorized access and use
- Monitoring and responding to security events and incidents in a timely manner
- Monitoring the performance of system components to support the needs of the system and system users
- Implementing data backup and restoration practices that support the availability of the system for system users
- Designing disaster recovery and business continuity procedures to support the continuity of company and system operations

Mural establishes operational requirements that support the achievement of security and confidentiality commitments and other system requirements. Such requirements are communicated in Mural'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 internal networks are managed, and how employees are hired and trained.