



Mersive Technologies

Report on Controls at a Service
Organization Relevant to
Security, Confidentiality, and
Availability

SOC 3[®]

For the Period March 1, 2025 to May 31, 2025

*SOC 3 is a registered service mark of the American Institute
of Certified Public Accountants (AICPA)*



Independent Service Auditor's Report

To the Management of Mersive Technologies ("Mersive"):

Scope

We have examined Mersive's accompanying assertion titled "Assertion of Mersive Management" (assertion) that the controls within Mersive's Mersive Collaboration Suite (the "system") were effective throughout the period March 1, 2025 to May 31, 2025, to provide reasonable assurance that Mersive's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, 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

Mersive 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 Mersive's service commitments and system requirements were achieved. Mersive has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Mersive 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 Mersive's service commitments and system requirements based on the applicable trust services criteria; and,
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Mersive'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.

Relevant Ethical Requirements

We are required to be independent of Mersive and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 Mersive's Mersive Collaboration Suite were effective throughout the period March 1, 2025 to May 31, 2025, to provide reasonable assurance that Mersive's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

July 15, 2025

Assertion of Mersive Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Mersive's Mersive Collaboration Suite (the "system") throughout the period March 1, 2025 to May 31, 2025, to provide reasonable assurance that Mersive's service commitments and system requirements relevant to security, confidentiality, and availability were achieved. Our attached system description of the Mersive Collaboration Suite identified 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 March 1, 2025 to May 31, 2025, to provide reasonable assurance that Mersive's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, 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). Mersive'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 the attached system description.

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 March 1, 2025 to May 31, 2025, to provide reasonable assurance that Mersive's service commitments and system requirements were achieved based on the applicable trust services criteria.

Mersive Technologies

July 15, 2025

Mersive's Description of the Boundaries of Its Mersive Collaboration Suite

Description of Services Provided

Mersive (the "company") provides collaboration software and hardware globally, launching a product in 2025 collectively referred to as the Mersive Collaboration Suite. The company was founded in 2006 and specializes in designing and deploying solutions that enable users to share and collaborate on content. The Mersive Collaboration Suite supports a wide array of applications, from small huddle rooms to large conference spaces, and enables wireless connectivity for content sharing from multiple devices.

The Mersive Collaboration Suite is structured into the following primary components:

- **Mersive Cloud Management Console**

- Cloud-based portal for managing MCS devices within a user's organization; and,
- Centralized management for settings which gives client administrators the ability to add users and control their access, and group devices into organizations that mirror the operational setup and needs of their business.

Additional services offered but outside of the scope of this report are structured into three primary components:

- **Mersive Smart**

- Software application for Android-based Smart TVs or streaming devices that enables cross platform collaboration for different workspace and teaming configurations.
- Connects directly to the display and network to receive and display content from various devices.

- **Mersive Essentials**

- Reflects the function of Mersive Smart, but includes a hardware component with the Mersive Gen4 Mini Pod that operates on a Linux Operating System to support secure wireless collaboration by connecting any display via HDMI.
- Leverages standard protocols such as Airplay and Google Cast in addition to the web-based content sharing application.

- **Mersive Pro**

- Includes a hardware component with the Mersive Gen4 Pod that operates on a Linux Operating System to support secure wireless collaboration by connecting any display via HDMI.
- Includes two USB-C ports to connect in-room peripherals (e.g., cameras, microphones).
- HDMI input for cable sharing between end-user devices and the Pod, audio input, Power over Ethernet port, DC power port, and dual HDMI 2.0 output for mirrored display.

Scope of the Report

The scope of this report covers the Mersive Cloud Management Console of the Mersive Collaboration Suite (the “system” or “Mersive Collaboration Suite”) and does not include Mersive’s software or hardware based appliances (i.e., Mersive SMART, Mersive Essentials, Mersive Pro).

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

Infrastructure

The system is hosted in Google Compute Platform (GCP) within an environment which protects the network from unauthorized external access through the use of firewall rules and access controls. User requests to Mersive web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote administration is secured through Identity and Access Management (IAM) controls and multi-factor authentication (MFA). The hardware components that make up the aforementioned system include servers hosted, managed, and protected by GCP. Production servers at GCP maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high availability data centers with multiple availability zones.

Software

Mersive is responsible for managing the development and operation of the Mersive Collaboration Suite including software components such as operating systems, databases, and storage systems, with exception to proprietary operating systems and databases that are managed by subservice organizations.

People

Mersive is organized in the following functional areas:

- **Executive Management:** Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives. Exercises oversight of the development and performance of internal control.
- **Engineering:** Responsible for the development, testing, and maintenance of the source code for the system. Also responsible for the product life cycle, including adding additional product functionality.
- **Cloud Operations:** Responsible for managing the production cloud environment, including deployments, monitoring, security, availability, backups, and system administration.
- **Information Security/Compliance:** Responsible for the following activities:
 - **Risk Management:** Includes assessing and responding to risk, monitoring internal and external security threats, communication of the annual risk assessment and control gaps to senior leadership, and third party due diligence.
 - **Control Oversight:** Includes monitoring and communication of regulatory changes, as well as subsequent control requirement changes and ongoing monitoring over the effective implementation of controls. Includes:

- **Security Committee/Governance Council:** Responsible for the annual review and approval of information security policies. This committee is composed of members of the executive and information security/compliance teams.
- **Human Resources:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **Finance:** Responsible for maintaining the accounting systems and ensuring their accuracy and timeliness.
- **Information Technology (IT):** Responsible for:
 - Managing laptops, software, and other technology involved in employee productivity and business operations;
 - Management of access, including account provisioning and deprovisioning;
 - Access management, including performance of access review controls and security; and,
 - Domain name management.
- **Customer Success:** Responsible for account management and customer support activities.
- **Sales and Marketing:** Responsible for promoting the business and mission of Mersive. Its key duties include defining and managing the products and services, conducting campaign management for marketing initiatives, and creating content.

Data

Data, as defined by Mersive, constitutes any information collected from employees, candidates, users, customers, vendors, or other parties that provide information to Mersive.

Information assets are assigned a sensitivity level based on the audience for the information. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

Classification Levels	Description	Examples of Data
Confidential	Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner or a company executive.	• User personally identifiable information (PII) • ePHI • Source code • Internal IPs • Anonymized usage data • Room names • Session names • OS information • Device metadata
Restricted	Proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.	• Application/Error logs
Public	Documents intended for public consumption which can be freely distributed outside Mersive.	• Product documentation posted on www.mersive.com/support

Processes and Procedures

Mersive has developed and communicated policies and procedures to manage the information security of the system. Policies are reviewed on an annual basis and changes are made to the policies when necessary. Policies are approved by the security committee/governance council on an annual basis. These policies and procedures cover the following key security life cycle areas:

- Access Control Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Plan
- Code of Conduct
- Cryptography Policy
- Data Management Policy
- Human Resource Security Policy
- Incident Response Plan (IRP)
- Information Security Policy
- Information Security Roles and Responsibilities Policy
- Operations Security Policy
- Risk Management Policy
- Secure Development Policy
- Third-party Management Policy

Principal Service Commitments and System Requirements

Mersive designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Mersive makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Mersive has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services. Mersive is also subject to state privacy security laws and regulations in the jurisdiction in which Mersive operates.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, status portals, blogs, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of security monitoring to prevent and identify potential security attacks from users outside the boundaries of the system;
- Firewalls to restrict system access from external and internal network; and,
- Annual penetration tests performed by an external third party.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Mersive and user entities.

Mersive establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations (such as DFARS), and other system requirements including the following:

- Confidentiality or non-disclosure agreements with employees and third parties with access to customer data.

Mersive establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Mersive'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 the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools accessible to all personnel with access to the company systems.