Mursion

System and Organization Controls (SOC) 3 Report on Mursion, Inc.'s Virtual Reality Training Platform System Relevant to Security, Confidentiality, and Privacy Throughout the Period January 1, 2021 to June 30, 2021

DiSanto Priest & Co.
Certified Public Accountants

Table of Contents

I. Independent Service Auditors' Report

To the Management of Mursion, Inc.:

Scope

We have examined Mursion, Inc.'s accompanying assertion titled "Mursion Inc.'s Management Assertion" (assertion) that the controls within Mursion, Inc.'s Virtual Reality Training Platform System (system) were effective throughout the period January 1, 2021 to June 30, 2021, to provide reasonable assurance that Mursion, Inc.'s service commitments and system requirements were achieved based on trust services criteria relevant to security, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Mursion, Inc. uses a subservice organization, to provide web services that host the Mursion, Inc. Virtual Reality Training Platform System. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mursion, Inc., to achieve Mursion, Inc.'s service commitments and system requirements based on the applicable trust services criteria. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Mursion, Inc. 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 Mursion, Inc.'s service commitments and system requirements were achieved. Mursion, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Mursion, Inc. 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 Auditors' 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 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 Mursion, Inc.'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 Mursion, Inc.'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 Mursion, Inc.'s Virtual Reality Training Platform System were effective throughout the period January 1, 2021 to June 30, 2021, to provide reasonable assurance that Mursion, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

DiSanto, Priest + Co.

November 4, 2021
Warwick, Rhode Island

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations
™

II. Mursion, Inc.'s Management Assertion

Mursion

We are responsible for designing, implementing, operating, and maintaining effective controls within Mursion, Inc.'s Virtual Reality Training Platform System (system) throughout the period January 1, 2021 to June 30, 2021, to provide reasonable assurance that Mursion, Inc.'s service commitments and system requirements relevant to security, confidentiality, and privacy (applicable trust services criteria) 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 January 1, 2021 to June 30, 2021, to provide reasonable assurance that Mursion, Inc.'s service commitments and system requirements were achieved based on the 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*).

Mursion, Inc.'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 January 1, 2021 to June 30, 2021, to provide reasonable assurance that Mursion Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Mursion, Inc.
November 4, 2021

Attachment A – Mursion, Inc.'s Virtual Reality Training Platform System

A. Overview of Services Provided

Mursion, Inc. (Mursion) provides training powered by a blend of artificial intelligence and live human interaction. Mursion provides immersive training for essential skills in the workplace. By using trained professionals who orchestrate the interactions between learners and avatar-based characters, Mursion simulations achieve the realism needed to deliver measurable, high-impact results. Applicable to any situation requiring high stakes interpersonal skills, the approach has demonstrated impact in areas such as leadership development, sales enablement, customer service, and diversity and inclusion, across industries. Authentic interactions simultaneously engage the emotional and cognitive faculties for learning that truly transforms the learner.

B. Relevant Aspects of the Overall Control Environment

A company's internal control environment reflects the overall attitude, awareness, and actions of management, and others concerning controls and the emphasis given to controls, as expressed by the Company's policies, procedures, methods, and organizational structure. The following is a summary of certain components of internal control pertaining to the Company's systems.

1. Control Environment and Control Activities

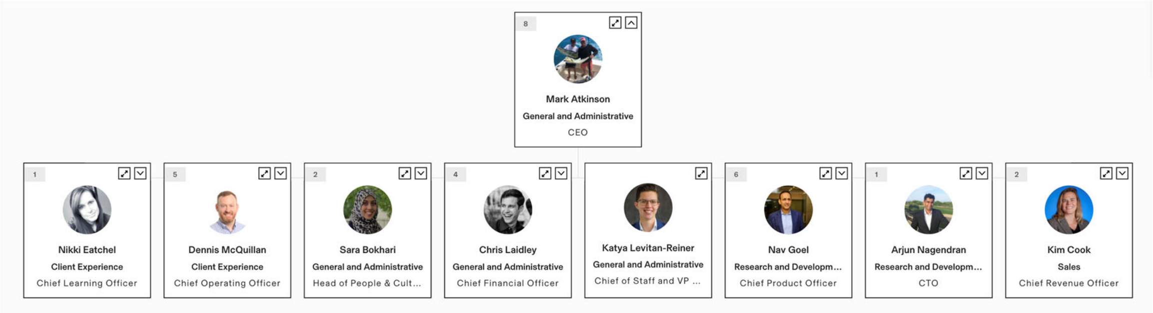
a. Management

Executive management believes every employee contributes to the success of the client, impacting both client retention and Mursion growth. The Company's management team is comprised of a diversely skilled and experienced group, ultimately responsible for the vision and direction of Mursion as a whole. These individuals meet bi-weekly to discuss a wide range of topics. They are also responsible for establishing corporate policy and addressing all operational, technical, financial, cultural, and social aspects of Mursion.

i. The Mursion Information Security Program defines the expectations that management has with regards to the security, confidentiality, and privacy of client data. Overall oversight is conducted through the Chief Technology Officer, who has general responsibility for the information technology (IT) systems and their security.

b. Organizational Structure

The following is a functional structure at the executive level of the Company. The entity maintains an up-to-date organizational chart defining responsibilities and reporting lines. The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system, enabling it to meet its commitments and requirements.



Mark Atkinson – Chief Executive Officer - Responsible for Mursion's long-term strategic plan, capital requirements, and key leadership positions. Mark has spent the last twenty years building technology ventures that support human capital development in K-12 education and corporate learning. Mark founded TeachForward, LLC, a full-service educational consulting firm with a proprietary web platform that delivers custom-developed, performance assessments to K-12 educators.

Arjun Nagendran – Chief Technology Officer - Arjun completed his Ph.D. in Robotics from the University of Manchester, UK, specializing in landing mechanisms for unmanned air vehicles. Prior to Mursion, he worked for several years as an academic researcher leading the ground vehicle robotic system for Team Tumbleweed, which was one of the six-finalists at the Ministry of Defense (UK) Grand Challenge. Arjun's current interests involve coupling machine learning, psychology and the learning sciences with technological advancements in remote-operation, virtual reality, and control system theory to create high-impact real world applications.

Nikki Eatchel - Chief Learning Officer - Nikki has built her career over more than 25 years in the assessment industry, serving in executive leadership positions in assessment development, psychometrics, business development, product and program management, customer support, documentation, training software development, and quality assurance (QA) for several leading global assessment organizations. Her responsibilities have spanned the full spectrum of assessment and learning activities, including research, assessment design and development, job analysis, global delivery, standardized scoring and reporting, and individual and organizational analytics. Nikki has been personally responsible for ensuring the validity and fairness of large-scale global programs as well as statewide assessment products and services.

Dennis McQuillan - Chief Operations Officer - Dennis leads the operational functions of Mursion, is responsible for the long-term global operating plan of the business, and ensures Mursion can consistently deliver exceptional service to clients. Earlier in his career, Dennis led operations for General Assembly's Enterprise business, spent five years at Deloitte Consulting in their Strategy & Operations group, and worked in finance for the Related Companies and Boston Scientific. Dennis holds a Master of Business Administration (MBA) from New York University Stern School of Business and a Bachelor of Science (BS) from Bentley University.

Sara Bokhari – Head of People and Culture - Sara champions Mursion’s culture and leads efforts in finding, developing, motivating, and retaining Mursion’s talented workforce. She transitioned to this role after serving as the Director of Education Services, where she worked with her team to build our robust simulation offerings for Higher Education and K-12 School Districts. Sara holds a MBA from The George Washington University, a Master of Arts (MA) in Education from Bank Street College of Education, and a Bachelor of Arts (BA) in Anthropology from the University of Illinois.

Chris Laidley – Chief Financial Officer - Chris is a strategic finance and operations executive with demonstrated ability to drive high-growth businesses towards scale. Before joining Mursion, he developed and implemented financial and operational strategies to scale EdTech start-up 2U from a team of 8 employees, through Initial Public Offering (IPO), to a global multi-product corporation with more than 6,000 full-time employees in six international markets. He was the lead member of the due-diligence and integration teams for two industry defining EdTech acquisitions - $110M for GetSmarter and $750M for Trilogy Education, and guided 2U through a successful IPO and two follow-on offerings that raised more than $630M of capital to fuel 2U’s rapid growth initiatives and multi product line expansion. In addition, Chris is an active board member for Archbishop Spalding High School based in the Baltimore metro area.

Katya Levitan-Reiner – Chief of Staff – Katya has served as Chief Operating Officer (COO) of Propel Capital, which invests in early-stage ventures and visionary leaders challenging the status quo and driving transformational change. Propel, founded in 2008, uses blended capital (political, investment, philanthropic) and invests 100% of its assets in alignment with its mission. Portfolios include Propel Democracy to build progressive power in the United States and Propel Opportunity to support economic opportunity and impact investing. Previously, Katya led her own consulting practice working with foundations, non-profits, and school systems and provided strategy and implementation support to Fortune 500 companies as part of the Human Capital practice at Deloitte.

Navneet Goel – Chief Product Officer - Nav leads Mursion’s Product Development, including product management and engineering. With more than 25 years of experience in product management, engineering management, and entrepreneurship, he has shipped products in many domains--enterprise, consumer, social, e-commerce, customer relationship management (CRM), cloud, and software as a service (SaaS). Nav holds a Bachelor of Engineering (BE) degree in Computer Science and Engineering from the Institution of Engineering and Technology (IET) India and a MBA degree from the University of California, Berkeley.

Kimberly Cook – Chief Revenue Officer (CRO) - Kim is a 25-year technology industry veteran with roots in traditional and digital media. She joins an extraordinary Mursion team as CRO with a vision to help uplift human interactions for better performance while overseeing the sales and marketing teams for this revolutionary startup. Kimberly is a graduate of Michigan State University and is a sought after speaker sharing experience on how technology impacts performance at leading global conferences.

c. Personnel

Mursion is committed to helping to ensure that all employees are competent to perform all required activities. To achieve this goal, Mursion conducts extensive candidate searches and background checks to recruit the best possible candidates for all positions and then provides the chosen candidates with the tools, training, resources, and leadership required to perform to the best of their abilities. Mursion has written job descriptions specifying the responsibilities and requirements for key job positions, specifically for personnel responsible for the design, development, implementation, and operation of systems affecting the security, privacy, and confidentiality of Mursion services.

As a condition of employment, screenings are performed on applicants and new-hires by an employment screening vendor:

- Appropriate background checks, including as appropriate and based on risk determination, criminal and credit checks
- Social security number trace
- Social security fraud detection
- National sex offender registry

In addition to the pre-employment screening, only personnel who meet the following criteria are granted access to Mursion systems:

- Have reviewed and signed the confidentiality agreement
- Require access to perform their job functions
- Have completed an internal approval process
- Have been subjected to background checks as noted above
- Have completed the security awareness training program and agreed to abide by the Acceptable Use Policy

To help ensure that employees are provided with appropriate career-guidance, employee's supervisors and managers are available for coaching and day-to-day guidance regularly. Where an employee is identified to fall short of expectations and job duties, appropriate corrective action is applied. Depending on the severity of the issue, actions can include counseling, training/re-training, and termination of employment. Similar actions are taken if an individual is found to have violated the Company's confidentially agreement or the Acceptable Use Policy.

Mursion has high expectations for all employees, and management can withdraw access from personnel if they have reason to believe that they are not complying with Mursion's Code of Business Ethics and Conduct, based upon ongoing monitoring of key processes and the results of periodic audits of logical access logs.

2. Risk Assessment

Mursion performs monthly internal and external vulnerability scans on critical systems aimed at identifying potential threats of disruption to System operations, which would impair systems security, privacy, and confidentiality. If necessary, Mursion applies appropriate mitigation strategies in a timely manner and updates applicable policies based on its assessment of the risks associated with the identified threats. In addition, annual risk assessments are conducted to identify IT risks across the enterprise. This assessment utilizes National Institute of Standards and Technology (NIST) guidance as the basis and includes changes to the IT risk assessment, new environmental security risks, changes to regulations and standards, and changes to user requirements. As part of the risk assessments, management tracks, prioritizes and discusses potential material security, confidentiality, and privacy issues related to Mursion's products and services. Identified risks are categorized by impact and severity, solutions are discussed, and steps are taken to reduce, accept, transfer, or eliminate the risks.

3. Monitoring

Mursion has network diagrams in place to capture all the system components that are part of the network and baseline configurations are in place to help ensure security, confidentiality, and privacy of the information assets. Mursion management monitors all access to the environment on an ongoing basis. During the process, reviews are conducted over potential inappropriate access and unusual actions. Whenever certain operational thresholds are reached, the monitoring system alerts Company personnel, who assess and review the log files as appropriate.

Mursion employees are responsible for monitoring their environment and for notifying Company management of suspicious activities. Whenever customers or Mursion personnel identify suspicious activity on the system, the Company notifies customers as appropriate.

A firewall is in place and is configured to monitor and restrict unauthorized inbound and outbound traffic. An intrusion detection system (IDS) is configured on the firewall and report on any intrusions identified.

Additionally, systems in the Mursion environment run an anti-virus software application with up-to-date virus definitions. Scans and virus definition database updates are performed automatically.

Mursion systems are implemented to monitor key operational metrics and to notify appropriate personnel when certain operational thresholds are reached. To help prevent and mitigate threats, the monitoring of these key operational metrics is automated. This monitoring includes but is not limited to, the following:

- Storage space
- CPU utilization
- Memory utilization
- Anti-virus alerts
- Login page privacy
- Environments operate in an N+1 state

In addition, Mursion management monitors regulatory and technology changes and considers their developmental and operational impact on Company systems on an ongoing basis.

Mursion also performs reviews over the risk assessment of its subservice organization at least annually to verify performance against contracted requirements and commitments, including those related to security, confidentiality, and privacy. As part of this risk assessment, Mursion reviews the available System Organization Controls (SOC) 2 reports for its subservice organizations and reviews a comprehensive vendor analysis report.

4. Risk and Vulnerability Management

Mursion performs monthly internal and external vulnerability scans on critical systems aimed at identifying potential threats of disruption to System operations, which would impair systems security, confidentiality, and privacy. If necessary, Mursion applies appropriate mitigation strategies in a timely manner and updates applicable policies based on its assessment of the risks associated with the identified threats. In addition, annual risk assessments are conducted to identify IT risks across the enterprise. This assessment includes changes to the IT risk assessment, new environmental security risks, changes to regulations and standards, and changes to user requirements. As part of the risk assessments, management tracks, prioritizes and discusses potential material security, confidentiality, and privacy issues related to Mursion’s products and services. Identified risks are categorized by impact and severity, solutions are discussed, and steps are taken to reduce, accept, transfer, or eliminate the risks.

The Chief Technology Officer and the IT Director meet monthly to provide oversight to Mursion's control environment. Specific responsibilities and duties include the following:

- Review risk registry containing all identified risks and ensure open issues are remediated in a timely fashion.
- Review policies pertaining to information security and cyber threats, taking into account the potential for external threats, internal threats, and threats arising from transactions with trusted third parties and vendors
- Review the framework to prevent, detect, and respond to cyber-attacks or breaches, as well as identifying areas of concern regarding possible vulnerabilities and best practices to secure points of weakness. Creating and executing action plans
- Review Company policies and frameworks relating to access controls, critical incident response plans, business continuity and disaster recovery, physical and remote system access, and perimeter protection of IT assets
- Review programs to educate Mursion employees about relevant information security issues and Mursion policies concerning information security
- Review reports regarding the results of reviews and assessments from the IT team, or other internal departments
- Review and approve Mursion's risk governance structure, including the risk management framework, policies and risk tolerances adopted by management
- Discuss the Company's significant risk exposures and review the steps management has taken to monitor and control such exposures, including Mursion's risk assessment and risk management policies
- Receive, as and when appropriate, reports and recommendations from management on Mursion's risk tolerance
- Review and approve Mursion's internal audit work plan to ensure alignment with identified risks and governance need
- Receive reports, when appropriate, regarding the results of risk management reviews and assessments from other internal departments as well as any third parties assisting Mursion with its information security responsibilities

5. Information and Communication

Mursion has implemented layered mechanisms of communication to employees to ensure that all workforce members understand their roles and responsibilities concerning the provision of services to clients and to promote timely communication of significant events. These methods include:

- Training provided upon hire and as needed or at least annually thereafter
- Notices to employees when needed to relay significant policy or organizational events and changes
- Monthly management meetings
- Written policies and standard operating procedures (SOP), which all employees are required to follow; are available, maintained, and secured via internal network access

6. Security Awareness and Training

Internally, Mursion personnel undergo a training program to learn about the Company's platforms. In addition, no less frequently than annually, all Mursion personnel take a Company-specific security awareness training, which incorporates training information related to the security, privacy, and confidentiality obligations of Mursion's information. If there are changes that could potentially affect any of the requirements noted above, security awareness training is updated accordingly. Employees can find IT security, privacy, and confidentiality policies on the Mursion shared drive. In addition to the security training, Mursion also performs internal phishing campaigns and phishing-specific user training to maintain a heightened level of employee awareness regarding attacks that originate via e-mail.

Responsibility and accountability for the Mursion's system security, confidentiality, and privacy policies are defined. They are communicated to personnel responsible for implementing them via Mursion's standard operating procedures and policy documentation. Any updates to the policies are reviewed at the executive level and implemented as appropriate.

7. Logical Access

Company Personnel Access

Mursion uses role-based groups to restrict access to system resources and restricts access to the resources to only the users granted permissions to that respective resource, based on job responsibilities. All Mursion users must authenticate to the network and application systems using a valid and unique user ID, which is authenticated by an associated password. All Mursion employees who require access to the Company's environment must complete security awareness training. Consultants and interns are assessed through security interviews and given appropriate training as needed.

Before being granted access to Mursion systems, personnel are subject to an internal approval process in which their roles are validated by senior management.

Mursion requires all user passwords for all in-scope applications and operating systems to meet the following minimum complexity requirements:

Be a certain number of characters in length and contain characters from the following categories:

- English lowercase characters (a through z)
- English uppercase characters (A through Z)
- Base 10 digits (0 through 9)

Users are locked out of the system after five unsuccessful attempts
Passwords are changed every ninety days

Reset lockout counter after four hours
Password history set to three passwords remembered

In addition, passwords are hashed using an industry-standard algorithm. Also, only the hashed values of passwords are stored. When passwords are entered, they are similarly hashed using the same algorithm, and the result is compared against the stored value.

Privileged/administrative access to infrastructure, systems, and technology components is limited to specific members of the IT team.

Access to the Mursion systems is revoked as a component of the termination process. Quarterly, inactive logical access accounts are identified and appropriately addressed through deletion or other means.

8. Physical and Environmental Security

Mursion restricts access to offices and wiring closets, and utilizes devices to protect from theft, misuse, and unauthorized access. Building access is monitored and only given to authorized personnel, and a security officer is posted at the building entrance at all times to monitor entry. Cameras, alarms, and IDS further protect against unauthorized entry and theft, and can also be used for surveillance during an environmental disaster event. The facility is equipped with fire-suppression systems, climate control and monitoring systems, and emergency backup power systems.

9. Application Development

Mursion has controls in place to verify that product is secured and stable before uploading it to the production server. The Company has a Systems Development Life Cycle (SDLC) that is published and disseminated across all developers. This policy requires personnel to inform management of any deficiencies identified during system operation and monitoring and to obtain approval of system changes that may affect system security, confidentiality, or privacy. Developer, staging, and production servers are separated to reduce bugs reaching the production server.

10. Data Handling

Mursion’s core scheduling product is multitenant, allowing control on datasets and safeguarding against cross-contamination of data. All clients are segregated on the server end by e-mail address.

Mursion has established a data classification matrix, which outlines the data lifecycle management system and is disseminated to all employees, as well as available on the internal Mursion shared drive where it is regularly referred to by the Company’s data processors. All data is classified, and a set retention period is created. The retention period is ingrained in the software, when able, and audited annually to ensure data is destroyed or retained, as listed. Security Information and Event Management (SIEM) device alerts security personnel when data classification is changed or removed. By design, all data is encrypted at rest and in transit, and the Mursion portal stores all data in a secured database that uses authentication tokens to authenticate users.

Mursion's privacy notice can be found at mursion.com/privacynotice and is updated by management at least annually to comply with international and local regulations. The privacy notice details the types of information collected, as well as the Company's basis for determining consent for the collection, use, retention, disclosure, and disposal of personal information. Personal information can be viewed or changed at any time by contacting the Company. Users of the system must explicitly consent to the video and audio recording of training sessions and the privacy notice prior to starting the training session.

Mursion data is stored on Amazon Web Services (AWS) to ensure the highest security standards are in place to protect data. Systems are backed up on the AWS servers on a daily basis and retained for thirty days.

11. Change Management

Mursion has documented change management policies that govern the addition, deletion, or alteration of any hardware, software, network, or telephony components or configurations in the Company infrastructure. All changes are thoroughly tested in a staging environment and require the approval of management before the release to production.

12. Incident Response

Mursion has a documented Incident Response Plan for the identification and mitigation of security and confidentiality breaches, privacy issues, and other incidents, including a defined process for staff members to submit complaints. Users are instructed to inform a member of senior management via phone or in-person of any potential issues.

When an incident related to systems security, confidentiality, and privacy policies is detected or reported, a defined incident management process is initiated by authorized personnel. A ticket is created to ensure tracking of the incident and resolution time are adhered to. Certain issues with regard to privacy are not tracked in the ticketing system to ensure anonymity for clients. These issues are tracked directly by the Company's appointed Data Protection Officer. Corrective actions are implemented per defined policies and procedures, and all incidents, including open incidents, are tracked by management in the documented plan of actions and milestones matrices until they are resolved. Closed incidents, including those addressing system security, confidentiality, and privacy, are reviewed by management for appropriate resolution.

When an incident occurs related to logical or physical security in relation to business continuity or disaster recovery, an incident response team will be appointed, depending on the nature of the incident, as outlined in the business continuity and disaster recovery plan.

For any confirmed incidents or significant updates that affect the security, confidentiality or privacy of customer data, including the handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information, specific Company personnel has been designated to communicate with customers, legal authorities, and the public as appropriate.

To help ensure that Mursion personnel are aware of incident response procedures, Mursion's security awareness training contains information concerning the identification of possible security and confidentiality breaches, privacy issues, and the process for informing the appropriate Mursion personnel of complaints.

Identified System Incidents

There were no identified system incidents from January 1, 2021 to June 30, 2021.

C. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions to improve operating and administrative effectiveness. This attachment includes only certain policies, procedures, and control activities at the Company. It does not include the policies, procedures, and control activities at the third-party service organization. The achievement of design related to the Trust Services Criteria assumes that complementary controls at the subservice organization that support these criteria are in place and operating effectively.

D. User Entity Responsibilities

In order for user entities of the Virtual Reality Training Platform System to derive the intended benefits of the system, the user entities have certain additional responsibilities. These user entity responsibilities may vary dependent upon the service and specific client needs. These user entity responsibilities will be documented in each client's contract, Company website, master service agreement, and in training.

Attachment B – Principal Service Commitments and System Requirements

Mursion's internal processes and procedures reflect the commitments Mursion makes to its clients as well as any applicable laws or financial, operational, and compliance requirements to which Mursion must abide with respect to the delivery of its services and performance of its operations. Security, Confidentiality, and Privacy terms are examples of these commitments and can be located in Mursion's Master Service Agreements and Statements of Work. They are also reflected in Mursion's internal processes and procedures. Such security, confidentiality and privacy commitments are standardized and include the following:

- The maintenance of an information security program that includes appropriate administrative, physical, and technical safeguards to prevent and guard against unauthorized access, disclosure, destruction, loss or alteration of client data.
- The use of identity access management software and controls for usernames and passwords, access provisioning and de-provisioning, and role-based access.
- The use of reasonable firewalls, boundary protections, anti-malware, and intrusion detection systems.
- The use of encryption technologies to protect customer data in transit.
- The establishment of operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements.
- Maximum retention periods for data collected during normal operations.
- Procedures for managing security incidents and breaches, including notification procedures.

These requirements are communicated in Mursion's system policies, procedures, design, documentation, and contracts. Information security, confidentiality and privacy policies define an organization-wide approach to how systems and data are protected. These include policies around how the systems are designed and developed, how the systems are 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 have been documented on how to carry out specific manual and automated processes required in the operation and development of the Virtual Reality Training Platform System.