Matterport™

Matterport LLC

System and Organization Controls (SOC) 3 Report

Report on Matterport LLC
Security, Availability, and Confidentiality

From the Period of February 1, 2024 to January 31, 2025

Frank, Rimerman + Co. LLP
certified public accountants

Table of Contents

Section I – Independent Service Auditor's Report 3
Section II – Assertion Provided by Matterport LLC Management 5
Attachment A – Matterport Cloud Service Description Provided by Matterport LLC 6
Attachment B – The Principal Service Commitments and System Requirements 11

Section I – Independent Service Auditor's Report

Matterport LLC
Sunnyvale, California

Scope

We have examined Matterport LLC's (the Company) management assertion in Section II of this report titled "Assertion Provided by Matterport LLC's Management" (the assertion) that the controls within the Company's Matterport Cloud Service (the Service) were effective throughout the period from February 1, 2024 to January 31, 2025, to provide reasonable assurance the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*.

Attachment A within this report, titled "Description of the Matterport Cloud Service," indicates subservice organization and complementary user-entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such subservice organization and complementary user-entity controls, and we have not evaluated the suitability of the design or operating effectiveness of the controls.

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Service to provide reasonable assurance the Company's service commitments and system requirements were achieved. The Company has also provided the accompanying assertion about the effectiveness of controls within the Service. When preparing its assertion, the Company 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 Service.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the Service were effective throughout the period from February 1, 2024 to January 31, 2025, to provide reasonable assurance the Company'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 AICPA. Those standards require us to plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe the audit evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the Service and the Company's service commitments and system requirements.
- Assessing the risks the controls were not effective to achieve the Company’s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the Service were effective to achieve the Company’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.

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

Our examination was not conducted for the purpose of evaluating the Company’s cybersecurity risk management program. Accordingly, we do not express an opinion on any other form of assurance on its cybersecurity risk management program.

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 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 the controls may become inadequate because of changes in conditions or the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion the controls within the Company’s Service were effective throughout the period from February 1, 2024 to January 31, 2025, to provide reasonable assurance the Company’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Frank, Rimerman & Co. LLP

San Jose, California
July 21, 2025

Section II – Assertion Provided by Matterport LLC Management

We, as the management of Matterport LLC, are responsible for:

- Identifying the Matterport Cloud Service (the Service) and describing the boundaries of the Service. Our description of the boundaries of the Service is presented in Attachment A, “Matterport Cloud Service Description Provided by Matterport LLC” and identifies the aspects of the Service.

- Identifying our principal service commitments and system requirements. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B within this report, titled “The Principal Service Commitments and System Requirements”.

- Identifying the risks that would threaten the achievement of our principal service commitments and system requirements that are the objectives of the Service.

- Identifying, designing, implementing, operating, and monitoring effective controls over the Service to mitigate risks that threaten the achievement of the principal service commitments and system requirements. In designing the controls over the Service, we determined that certain trust services criteria can only be met if complementary user- entity controls are suitably designed and operating effectively throughout the period from February 1, 2024 to January 31, 2025.

- Selecting the trust services categories and associated criteria that are the basis of our assertion.

We confirm to the best of our knowledge and belief that the controls over the Service were effective throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in the AICPA’s TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, and if user-entity controls assumed in the design of the Company’s controls throughout the period from February 1, 2024 to January 31, 2025.

Matterport LLC

/s/ Japjit Tulsi
Chief Technology Officer
July 21, 2025

Attachment A – Matterport Cloud Service Description Provided by Matterport LLC

Matterport LLC (The Company or Matterport) is a Software-as-a-Service company that provides the Matterport Cloud Service (the Service), which enables users to capture and connect to images of rooms, facilities, and construction worksites to create truly interactive 3D models of physical spaces. Matterport's proprietary Artificial Intelligence (AI) technology automatically creates a dimensionally accurate, photo-realistic 3D models of any structure. Matterport's spatial data provides building insights and analysis, allowing users to have a more efficient and scalable way to experience and manage physical spaces. A user can access the Service portal with their login credentials.

The Service provides customers the following in-scope features:

- Matterport Cloud: cloud hosting, processing, and space and user management;
- Matterport 3D model and add-on features: to capture physical space; and
- Matterport 3D Showcase Player: a web-based viewer enabling users to visualize and navigate through their 3D model of the physical space.

Matterport also provides Pro 3D cameras to capture visual and spatial data and the appearance and dimensions of space. The Pro 3D cameras are outside of the scope of this examination.

Matterport enables users to:

- Manage digital copies of real-world assets;
- Leverage spatial datasets to create new services;
- Provide a collaborative platform through a secure dashboard to manage 3D models; and
- Document interactions and collaborate efficiently with teams.

Components Used to Provide the Service

The boundaries of the Service are the specific aspects of the Company's infrastructure, software, people, processes and procedures, and data necessary to provide its services. Any infrastructure, software, people, and data indirectly supporting the services provided to customers by Matterport are not included within the boundaries of the Service. The components directly supporting the services provided to the customers are described below.

Infrastructure

The Service is based on a multi-tenant architecture that applies common and consistent management processes and controls to customers. The Service infrastructure is hosted and managed by Amazon Web Services, Inc. (AWS). The Matterport infrastructure is located in the AWS US-east-1 region and configured across multiple availability zones to ensure fault tolerance, high availability, and disaster recovery.

Databases are deployed in multiple availability zones, each with fully redundant power, networking, and connectivity housed in separate, secured facilities. Administrative access to AWS infrastructure is strictly controlled and monitored through a bastion host with a host-based intrusion detection system.

AWS is responsible for operating, managing, and controlling various components of the virtualization layer and storage, as well as the physical security and environmental controls. Through daily operations, the Company monitors the quality of AWS's performance. Controls operated by AWS are not included in the scope of this report.

Software

The Service utilizes custom-developed and externally supported software tools and services.

- Atlassian’s Jira is used to plan, track, and manage all of Matterport’s infrastructure and software development projects through the change management process.
- GitHub Enterprise is a source code control repository that hosts and stores Matterport’s source code and development projects and includes review and approval workflows for all Service code commits. Dependency Track is integrated with GitHub Enterprise to continuously inspect the software libraries packaged for vulnerabilities.
- Terraform is an open-source infrastructure-as-code software used to build and version production infrastructure, ensuring all changes are auditable, automated, testable, and authorized through Matterport’s change management process.
- Jenkins is an open-source, automation server plugin ecosystem used to support the Matterport source code delivery pipelines.
- Datadog monitors the overall health and availability of the production environment.
- SentinelOne provides real-time vulnerability detection and alerting of all critical points of the Matterport infrastructure.
- Site24x7 and Datadog monitor the external availability of the Service.
- Cloudflare provides content delivery network services and Distributed Denial-of-Service, complete application security, and bot protection for the Service.

People

The organizational structure at the Company provides a framework for planning, executing, and controlling business operations. It starts with management and is supported by key department managers and team members to ensure the segregation of duties concept is applied across the Company with mitigating controls for support. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, and efficiency of operations.

The Company follows a structured onboarding process to familiarize new personnel with the Company’s processes, systems, security, practices, policies and procedures.

Data

Customer data includes customer personal data, and all data provided by customers to Matterport directly or through the Service, including the customer's account, payment information, products purchased, location, email address, financial, and other transaction data. There are two subtypes of customer data collected within the Service: Customer image data and customer personal data.

- Customer image data includes any content or data that customers upload to the Service. Customer image data may be considered confidential, based on customers' or authorized users' specifications of customer image data as restricted or private.
- Customer personal data is data classified as such under applicable data protection laws and considered confidential in accordance with such laws.

All data used in the Service is encrypted in transit and at rest using industry-recommended protocols, algorithms, and key sizes. The Company ingests user-submitted data, which may include PII, through a secure web interface using Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS). Authentication and session data are transmitted using Virtual Private Network (VPN), TLS, or secure shell (SSH) with applicable access control policy enforcement.

Procedures

The policies and procedures are a series of documents that are used to describe the controls implemented within the Company. The purpose of the policies and procedures is to describe the operating environment and define the practices performed on behalf of the customer. These procedures are divided into two high-level categories: manual procedures and automated procedures. Manual procedures are performed by personnel, whereas automated procedures are performed by computer software. The Company has automated procedures for monitoring performance, uptime, availability, and security events and alerting Company personnel. The Company has also developed and documented procedures for investigating and responding to potential security incidents that are tracked in the internal ticketing system. The policies and procedures include risk management, information security, information assets management, security and vulnerability management, and data classification and handling, among others. The policies and procedures are available to all Company personnel.

Control Environment

The Company's internal control environment is governed and managed by the Company's Board of Directors (the Board), management, and other personnel working on the achievement of objectives related to the effectiveness and efficiency of the Company's operations while following applicable laws and regulations. A Security Steering Committee meets with the Board periodically to communicate the current state of the business, including security and compliance-related updates.

Management emphasizes the implementation and adherence to controls and ethical behavior throughout the Company. The overarching business principles and standards of conduct contained within the Employee Handbook define the core values of the integrity expected of personnel. These principles are supported by a set of Company-wide commitments, standards, and requirements defining how the Company is governed. The Company has also developed a set of security-related policies as well as operational procedures outlining Company requirements to protect and secure assets and data and to hold individuals accountable for their internal control responsibilities. The Company has established policies and practices related to employee recruiting, hiring, onboarding, training, and performance evaluation. The HR team ensures third-party background checks are performed and new hires are aware of their obligation to protect the Company's information and customer data. Formal performance reviews are conducted annually to aid in the continuous improvement process for the employee and the control environment.

Communication and Information

Management is committed to maintaining effective communication with personnel, customers, and business partners. The Company has established security, availability, and confidentiality-related policies that note the roles, responsibilities, and overall rules for achieving the Company's information security goals. Company personnel participate in the security awareness training ensuring their awareness of Company policies.

The Company informs customers of the Company's commitments to the security of the Service and the confidentiality of the data stored within the Service within Cloud Subscription Agreement (CSA), Platform Subscription Agreement (PSA) or customized contracts. The Company's website contains the Service description and tutorials describing the features and functionality of the Service.

Risk Assessment

The Company understands the necessary balance between risk and control, and the intent of risk management is to reduce risk to an acceptable level. The Company attempts to reduce business risk through an annual information security risk assessment, where management identifies critical assets, the threats facing those assets, and the likelihood and impact of the security of the assets that could be compromised. Management reviews applicable laws and regulations, and the impact of new laws and regulations on the Company, as well as risks related to significant changes in production systems, key personnel, or operational environment. Risks are reviewed, assigned an owner, and remediated within a timeframe based on criticality and Service impact.

Monitoring

The Company has designated a team responsible for monitoring the effectiveness of internal controls in the normal course of business operations. Monitoring tools are used to identify anomalies and issues, as well as to detect intrusions and vulnerabilities. Deviations in the operations of internal controls, including security and availability events, are reported to management. In addition, any customer issues are communicated to the appropriate personnel for triaging and resolution.

Management engages a third-party consultant to conduct an internal audit of the Company's internal controls. When changes to internal controls occur, they are evaluated, agreed upon by the control owners, documented, and communicated in the Company's internal workspace. Results from the internal control reviews are communicated to management.

Complementary User-Entity Controls (CUECs)

Security and confidentiality is a shared responsibility between the Company and its customers. The Service was designed with the assumption that certain controls would be implemented by the customers (user entities). Certain requirements can be met only if the CUECs are suitably designed and operating effectively, along with related controls at the Company. Service users should consider whether the following controls have been put into operation at their organizations:

User entities are responsible for:
Ensuring content is legal, does not infringe any intellectual property rights, and is authorized, including private information displayed in any physical location that is captured in raw picture data.
Complying with all applicable laws, rules, and regulations.
Providing Matterport with complete and accurate information for the Service, including billing and payment information, and keeping such information up to date with Matterport.
Complying with the Terms of Use and contractual agreements to prevent unauthorized access to or use of the Service.
Maintaining the security of login information, including passwords, associated with the Service.
Disallowing access to the Service to any person who is not an authorized user.
Performing periodic reviews of user access to the customer account.
Notifying Matterport immediately of any unauthorized access or illegal use of any login information.
Classifying Customer Image Data within the Service as public, private, or restricted, according to the customer's data classification policy.

Attachment B – The Principal Service Commitments and System Requirements

The Company makes service commitments to its customers and has established system requirements as part of the Service. Some of these commitments are principal to the performance of the Service and relate to the AICPA TSC relevant to the applicable trust services criteria. The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Service to provide reasonable assurance that its service commitments and system requirements are achieved based on the applicable trust services criteria.

Service commitments to customers are documented and communicated in written customer contracts, including the Cloud Subscription Agreement (CSA), Platform Subscription Agreement (PSA), or customized contracts. Service commitments include but are not limited to security, availability, and confidentiality.

Availability

The Company has made commitments related to percentage uptime and connectivity for the Service, as well as commitments related to service credits for instances of downtime.

The Company is architected its Service to maintain the availability through defined programs, processes, and procedures. Contingency plans and incident response procedures are maintained to reflect emerging continuity risks and lessons learned. Plans are tested, updated through the course of business, reviewed annually, and approved by management.

Security and Confidentiality

The Company has made commitments related to securing and maintaining the confidentiality of customer data and complying with relevant laws and regulations. These commitments are addressed through measures including confidentiality terms, data encryption, authentication mechanisms, and other relevant security controls.

The Company has also implemented technical controls designed to prevent unauthorized access to or disclosure of content. Internally, confidentiality requirements are communicated to employees through training and policies. Company personnel are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' data. In addition, the Company monitors the third parties used to support the Service through annual periodic reviews by evaluating performance against contractual obligations, including confidentiality commitments.

The Company has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are documented in the Company system policies and procedures, system design documentation, and contracts with customers.

Information security policies define a Company-wide approach to how systems and data are protected. These policies include how the Service is designed, developed, and operated, how the internal business systems and networks supporting the Service 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 various services provided by the Service.