Matterport Technical and Organization Security Measures
(Annex II To Matterport's Standard Contractual Clauses)

Updated: April 1, 2022

Matterport's technical and organizational security measures ("TOM") describe the controls implemented by Matterport to protect personal data and ensure the ongoing security, confidentiality, integrity, and availability of Matterport's products and services as described in any customer Agreement (the "Services").

I. Overview.

This document is a high-level overview of Matterport's TOMs. More details on the measures we implement are available upon request. Matterport reserves the right to modify or revise these TOMs at any time at its discretion without notice, provided that such modification or revision does not result in a material degradation in the protection provided for personal data that Matterport processes in providing its various Services.

Evidence of the measures implemented and maintained by Matterport described below may be provided to the customer, upon written request. Matterport will provide such evidence no more than once per year, in the form of up-to-date attestations, reports or extracts from independent bodies. Customers may also request at any time Matterport's Trust Package, which includes the most recent SOC2 Type II report, and the latest penetration testing report by visiting Matterport's Trust Center located at https://matterport.com/trust.

II. Shared Responsibility.

Matterport's TOMs apply to all standard service offerings provided by Matterport, except for those areas where the customer shares the responsibility for security and privacy TOMs.

Matterport adopts a shared responsibility model where responsibility for data security is shared between Matterport and the customer. This shared model can help relieve the customer's operational burden.

Matterport is responsible for protecting the infrastructure that runs all the Services offered within Matterport's cloud Services. This infrastructure is composed of the hardware, software, networking, and facilities that run the cloud-based Services. Matterport operates, manages, and controls the components from its host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Matterport hosts all its applications with Amazon Web Services (AWS) in a multi-tenancy environment. This allows Matterport to deploy, at scale, its code base to all its infrastructure, so the Services can serve multiple customers. Matterport currently does not support single-tenancy environments. Customer is responsible for the management of the user accounts, and visibility of its models. Customer may have additional responsibilities depending on the type of cloud Services that a customer selects. The type of cloud Services determines the amount of configuration work the

customer must perform as part of its security responsibilities.

III. Technical and Organizational Measures.

Matterport maintains the following TOM to protect personal data:

1. **Information Security Program.** Matterport will maintain organizational, management and dedicated staff responsible for the development, implementation, and maintenance of Matterport's information security program.

2. **Security Policies**. Matterport will maintain information security policies and make sure that policies and measures are regularly reviewed and amend such policies as Matterport deems reasonable to maintain protection of Services and data processed therein.

3. **Risk Management.** Matterport will assess risks related to processing of personal data and create an action plan to mitigate identified risks. Matterport will maintain risk assessment procedures for the purposes of such periodic review and assessment of risks to the Matterport organization, monitoring and maintaining compliance with Matterport policies and procedures, and reporting the condition of its information security and compliance to senior internal management.

4. **Physical Security**. AWS maintains physical and environmental security of Matterport's Infrastructure containing customer confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Matterport facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

5. **System and Network Security.**

- **Network Security.** Matterport will maintain network security controls such as firewalls, remote access control via virtual private networks or remote access solutions, network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring, designed to protect systems from intrusion and limit the scope of any successful attack.

- **Data Security**. Matterport will maintain data security controls which include logical segregation of data, restricted (e.g., role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.

- **Encryption**. Matterport employs encrypted and authenticated remote connectivity to Matterport computing environments and customer systems. Matterport maintains a cryptographic standard that aligns with recommendations from industry groups, government publications and other reputable standards groups. This standard is

periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

In-Transit Encryption. All network traffic flowing in and out of the Services data centers, including customer data, is encrypted in transit.

At-Rest Encryption. Customer data created by the customer, is encrypted at rest with 256-bit AES encryption.

6. **User Access Management**. Matterport will maintain logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

- Password Management. Matterport will maintain password controls designed to manage and control password strength, expiration, and usage including prohibiting users from sharing passwords. Matterport shall ensure password hardening standards are in place that align with accepted industry security frameworks to ensure sufficient controls.

- Workstation Protection. Matterport will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring screen lock timeout, malware software, firewall software, remote administration, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations. Matterport will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

- Media Handling. Matterport will implement protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures will be implemented for mobile computing devices to protect personal data.

7. **Auditing and Logging.** Matterport will maintain system audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review. Matterport will create, protect and retain such log records to the extent needed to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity, including successful and unsuccessful account logon events, account management, events, security events, object access, policy change, privileged functions, administrator account creation/deletion and other administrator activity, data deletions, data access and changes, firewall logs, and permission changes.

8. **Change Management.** Matterport will maintain change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Matterport technology and information assets. Any modifications to applications by Matterport (or a third party) that will create a major change or discontinuity – other than modifications linked to corrective maintenance – will be communicated to customers before being put into production so that customer may take the necessary measures to address any such discontinuity.

9. **Threat and Vulnerability Management.** Matterport will maintain measures meant to regularly identify, manage, assess, mitigate and/or remediate vulnerabilities within the Matterport computing environments. Measures include:

- Patch management
- Anti-virus / anti-malware
- Threat notification advisories
- Vulnerability scanning (all internal systems)
- Annual penetration testing (Internet facing systems) within remediation of identified vulnerabilities by a third-party security firm.

10. **Security Incidents**. Matterport will maintain incident response procedures designed to allow Matterport to investigate, respond to, mitigate, and notify of events related to Matterport technology and information assets. Matterport will follow documented incident response procedures to comply with applicable laws and regulations including data breach notification to any Data Controller, without undue delay, but in any event within forty-eight (48) hours, after Matterport's validation of a personal data breach known or reasonably suspected to affect customers' personal data.

11. **Business Continuity Plans.** Matterport will maintain defined business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and recovery from foreseeable emergency situations or disasters, consistent with industry standard practices.

12. **Vendor Management.** Matterport maintains a formal vendor management program, including vendor security reviews for critical vendors, to ensure compliance with Matterport's information security policies. Matterport may engage and use vendors, acting as sub-processors, that access, store, or process certain customer data. Matterport maintains updated information on its sub-processors on its website at https://matterport.com/matterport-subprocessors

13. **Privacy by Design.** Matterport will incorporate Privacy by Design principles for systems and enhancements at the earliest stage of development as well as educate all employees on security and privacy annually.

14. **Security of Disposed and Retained Data.** Matterport retains operational procedures and controls for the secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Matterport possession. Matterport retains back-up data in cloud storage for seven (7) days and may retain other data in accordance with applicable laws pursuant to Matterport's internal retention policies.