Matterport Security Schedule
Technical and Organizational Measures

Updated: March 20, 2024

These Contractor Technical and Organizational Measures for Security ("TOMS") are incorporated into the Agreement and describe the minimum controls required by Contractor to protect personal data and ensure the ongoing security, confidentiality, integrity, and availability of the Services and/or Deliverables as described in the Agreement. Contractor shall maintain the following TOMS to protect personal data:

1. **Information Security Program**. Contractor will be responsible for the development, implementation, and maintenance of Contractor's information security program.

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

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

4. System and Network Security.

4.1. **Data Security**. Contractor 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.

5. Contractor Personnel.

5.1. **Background Checks**. Contractor will ensure successful completion of background investigations of each of its personnel who may provide services to Matterport under the Agreement or any SOW or who may have access to any of Matterport's Confidential Information or Inventions. Background investigations shall include, at a minimum, verification of prior employment and criminal background checks, to the extent permitted by law, at the federal, state and local.

5.2. **Confidentiality Agreements**. Contractor will ensure adherence to confidentiality agreements for all personnel that will provide services to Matterport under the Agreement or any SOW or who will have access to any of Matterport's Confidential Information or Inventions.

5.3. **Security Awareness Training**. Contractor will ensure successful completion of security awareness training for itself and all personnel that will provide services to Matterport under the Agreement or any SOW or who will have access to any of Matterport's Confidential Information or Inventions.

6. **User Access Management**. Contractor will maintain the following 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).

    6.1. **Password Management**. Contractor will maintain password controls designed to manage and control password strength, expiration, and usage including prohibiting users from sharing passwords. Contractor shall adhere to password hardening standards that align with Matterport's accepted industry security frameworks to ensure sufficient controls.

    6.2. **Workstation Protection**. Contractor 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. Contractor will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

    6.3. **Media Handling**. Contractor 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.

    6.4. **Secure Messaging**. Contractor will use and maintain secure messaging and call language based on generally accepted industry standards.

7. **Auditing and Logging**. Contractor will maintain system audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review. Contractor 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**. Contractor will maintain change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to its technology and information assets.

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

9.1. Patch management

9.2. Anti-virus / anti-malware

9.3. Threat notification advisories

9.4. Vulnerability scanning (all internal systems)

9.5. Annual penetration testing (Internet facing systems) within remediation of identified vulnerabilities by a third-party security firm. During the term of the Agreement, an annual penetration testing report must be provided upon Matterport's request.

10. Security Incident Management

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

10.2. **Security Incident Reporting.** Contractor shall at its sole expense, make any notifications of a breach to the extent, to the persons or media outlets, at the time, and in the manner it is required to do so under applicable privacy and/or data security laws and regulations. Contractor shall promptly notify Matterport of any request by law enforcement official or agency to delay breach notification and, if the request was in writing, provide Matterport a copy of the request.

10.2.1. For any Matterport data or service affected by the security incident or breach, Contractor shall obtain Matterport's approval of the content of any breach notification before sending it, which approval shall not be unreasonably withheld.

10.2.2. Contractor shall provide reasonable cooperation and information reasonably requested by Matterport:

10.2.2.1. To facilitate Matterport's of the security risks arising from or associated with a security incident or breach, and

10.2.2.2. To facilitate compliance with Matterport's notification obligations if Matterport informs Contractor that it has its own requirement under applicable privacy and/or data security laws and regulations to provide notifications of a breach.

11. **Business Continuity Plans**. Contractor 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**. Contractor may engage and use vendors, acting as sub-processors, that access, store, or process certain customer data. Contractor agrees to maintain a formal vendor management program, including vendor security reviews for critical vendors, to ensure compliance with Contractor's information security policies. Contractor agrees to maintain a documented list of its sub-processors and it is provided for review by Matterport.

13. **Security Certifications**. Contractor shall obtain and provide security certifications and reports specific to the Services provided. Some examples of security certifications and reports include a SOC1/SOC2 report or ISO 27001 certification.

14. **Security of Disposed and Retained Data**. Contractor will maintain 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 Contractor's possession. Contractor agrees to maintain back-up data in cloud storage for at least seven (7) days and may retain other data in accordance with applicable laws pursuant to Contractor's internal retention policies.

15. **SOX Compliance**. Contractor will (1) promptly notify Matterport if: (i) has impacted or reasonably could impact the maintenance of Matterport's financial integrity or internal controls, the accuracy of Matterport's financial, accounting or human resource records and reports; or (ii) has had, or reasonably could have, any other material adverse impact on the applicable Services, Deliverables or the impacted business operations of Matterport and (2) promptly take corrective action to rectify (a) any error identified in any such report that could reasonably be expected to have an adverse impact on the Services or Deliverables and (b) any control deficiencies identified in the report.

` **IN WITNESS WHEREOF**, each of the Parties has caused this Security Schedule to be executed by its duly authorized representative:

MATTERPORT, INC.	**[counterpartyName_9mLnVpW]**
By:[matterportIncSignerSignature_cmxazPp]	By: [counterpartySignerSignature_eZZgsPZ]
Name: Nicole Joy Elmgart	Name:[counterpartySignerName_xK3fbp3]
Title: Director Legal, Head of Privacy	Title:[counterpartySignerTitle_mDQxRiu]
Date: [matterportIncSignerDateField_FPICjB4]	Date: