Vendor Security Requirements Addendum

Version March 1, 2023

This Vendor Security Requirements Addendum ("**Addendum**") is current as of the version date set forth above and shall remain in effect until and unless it is superseded at this same (or redirected) URL by a version with a later version date, and is hereby incorporated into and forms a part of the mutually executed agreement (the "**Agreement**") between Opendoor Labs Inc. and/or its affiliates ("**Opendoor**") and the service provider ("**Vendor**") for the provision of certain services (the "**Services**") by Vendor to Opendoor. In the event of any conflict between this Addendum and the Agreement, the terms of this Addendum shall prevail. Capitalized terms that are not defined in this Addendum shall retain the meaning ascribed to them in the Agreement.

1. Compliance.

1.1. Security Policies & Program. Vendor shall implement and maintain a comprehensive privacy and information security policy (the "**Security Policy**") that clearly defines Vendor's responsibility for the protection of any information made available to Vendor by Opendoor ("**Opendoor Information**"), including, without limitation, all Opendoor data and any information deemed confidential pursuant to the Agreement. In the event that Vendor makes a material change to the Security Policy, Vendor shall provide the updated Security Policy to Opendoor.

1.2. Compliance with Law. Vendor shall comply with all applicable federal, state, and international laws, rules, ordinances, statutes, decrees, and regulations related to data protection and consumer privacy (collectively, "**Data Processing Laws**").

1.3. Personnel. Vendor represents and warrants that Vendor and its employees, contractors, subcontractors, sub-processors, consultants, and agents (collectively, "**Personnel**") shall at all times comply with this Addendum (the "**Requirements**"), Data Processing Laws, the Security Policy, and the Security Program (as such term is defined below). Vendor shall provide annual Security Program and Security Policy training for its Personnel in addition to any other role-specific security training for Personnel relevant to their business function. To the extent Vendor utilizes sub-processors in the performance of services, Vendor shall publish a list of all such third party companies with access to its customer's information on its website. Vendor shall be fully liable for any and all damages resulting from its Personnel's violation of the Requirements, Data Processing Laws, or the Security Policy.

2. Access Controls.

2.1. Security Program. Vendor shall implement and maintain a comprehensive written information security program that (i) complies with all Data Processing Laws, (ii) contains reasonable and appropriate administrative, technical, organizational, and physical procedures and safeguards to preserve and protect the security, integrity, and confidentiality of systems, information, and data from and against unauthorized or unlawful acquisition, disclosure, processing, use, loss, destruction damage or alteration, and (iii) requires access to Opendoor Information, particularly sensitive Opendoor Information, be granted on a need-to-know basis, which is regularly assessed for validation by Vendor (the "**Security Program**"). In the event that Vendor makes a material change to the Security Program, Vendor shall immediately provide the updated Security Program to Opendoor.

2.2. Background Checks. Vendor must ensure that Personnel with access to Opendoor Information or Opendoor systems have passed basic background checks designed to validate such Personnel's resumes, professional qualifications, identity, and, where permitted by law, criminal history records. Personnel whose background checks reveal inconsistencies or convictions related to computer crimes, fraud, or theft must not be permitted to provide any portion of the services delivered to Opendoor pursuant to the Agreement.

2.3. Physical Security and Environmental Controls**.** Vendor will implement controls within its premises to restrict physical access to areas containing equipment used to facilitate the services pursuant to the Agreement, such as equipment used to access Opendoor Information. Such controls shall include, without limitation, layered perimeter controls and interior barriers, managed access to keys, entry and exit logs, and an appropriate response plan for intruder alerts.

2.4. Identification and Authentication.

a. *User Accounts*. Vendor will ensure that all user accounts used to provide Vendor's services are unique and are clearly associated with an individual user. Vendor will not allow group or "generic" accounts shared by many users on systems used to provide Vendor's services unless there is a pre-approved business need and such accounts are created in accordance with the Security Policy.

b. *Passwords*. All passwords utilized by Vendor's Personnel shall comply with sufficient complexity and expiration requirements as well as multi-factor authentication. Vendor shall require all passwords be stored in a hashed and salted format using a memory-hard or CPU-hard one-way hash function. Vendor's password and security requirements shall also enforce appropriate account lockout and brute-force protection on account access.

c. *Authentication*. Vendor must use multiple authentication factors and, at the very least, Two-Factor Authentication (as such term is defined below) when providing or using Data Hosting Services (as such term is defined below). For purposes of this Addendum, "**Two-factor Authentication**" shall mean the verification of a person's identity through the combination of (i) information known specifically by an individual, such as a username and password, and (ii) a separate identifier, such as a disconnected authentication token or a biometric factor like a fingerprint.

2.5. Network Access Controls. All networks utilized by Vendor to provide the services must be protected through the use of controls capable of blocking unauthorized network traffic, both inbound and outbound (ingress and egress). These devices must be configured to log network activity for audit, incident response and forensic purposes.

2.6. Segregation & Deletion of Opendoor Information. Vendor shall implement and maintain a comprehensive written data retention policy for Opendoor Information. Any Opendoor Information which Vendor stores must be logically segregated from all other Vendor data, Vendor's other Opendoor accounts, or any third-party data. Vendor must be able to delete Opendoor Information, including any backups, in its possession or control upon receipt of a written request from Opendoor and/or upon termination of the Agreement. Vendor's data sanitization efforts shall adhere to NIST SP 800-88 ***OR*** comparable standards when deleting Opendoor Information.

2.7. Inactivity. All Vendor devices must be locked after a reasonable period of inactivity. Accounts used by the Vendor to provide Vendor's services must be identified and disabled after a reasonable period of inactivity.

2.8. Termination of Personnel. Within twenty-four hours of the termination of Personnel, the terminated Personnel's access to the networks, systems, and accounts used to provide Vendor's services as well as any access to any Opendoor Information must be terminated.

3. Security Operations Management.

3.1. Vulnerability/Patch Management. Vendor will establish a commercially reasonable vulnerability/patch management process that ensures all systems used by Vendor to provide its services are promptly patched against any known security vulnerability within no more than ninety (90) days after Vendor's discovery of such security vulnerability.

3.2. Secure System Configuration. Vendor will establish commercially reasonable controls to ensure that all systems used to provide the services set forth in the Agreement are securely configured in a repeatable manner. This includes, without limitation, changes to default settings to improve system security (e.g., system "hardening"), changes to default account passwords, and removal of unnecessary software or services/daemons. Vendor must ensure sufficient employee device security configuration/features are in place such as Login Password, Anti-Virus, Full/Whole Disk Encryption, Administrative Privileges, and Firewalls.

3.3. Malware Prevention. Vendor will implement detection and prevention controls designed to protect against malicious software and appropriate user awareness procedures. Vendor will keep and update technical controls and must regularly evaluate all systems for the existence of malware. Vendor will run real-time or regular scans of Vendor's network and systems to detect viruses, malware, and possible security incidents.

3.4. Logging and Auditing.

a. *Generally*. Subject to the capabilities of the underlying application, database, or operating system, Vendor will capture activity logs for the following events: (i) modification (add, change, delete) to any named or user-accessible system resource; (ii) creation and deletion of resources; (iii) invalid user authentication attempts; (iv) successful accesses to security-critical system resources; (v) changes to users' security profiles, privileges, or attributes; (vi) changes to access rights of resources; (vii) changes to the system security configuration; (viii) modification of system-supplied software; (ix) program execution; and (x) mounting or dismounting any removable or remote data storage (i.e., tape, CD-ROM, floppy, NFS).

b. *For Data Hosting Services*. To the extent Vendor provides data hosting services ("**Data Hosting Services**"), Vendor will configure all its systems used to provide Data Hosting Services to ensure relevant information about actions performed by users or processes performed by the system for users are logged sufficiently to provide accountability. Logging will, at a minimum, include the following: (i) date and time of each logged event; (ii) source and destination IP address; (iii) user ID; (iv) services being invoked/executed (i.e., FTP, SSH, etc.); (v) the time that the session ends; and (vi) description of the event.

c. *Sensitive Data Elements*. Vendor will configure logging so it does not capture and record sensitive data elements, such as credit card data or authentication credentials (e.g., passwords).

d. *Card-processing systems*. To the extent Vendor provides services requiring credit card-processing, Vendor will configure payment card-processing systems to adhere to the PCI Data Security Standard (PCI-DSS) to the extent such requirement is applicable to the services provided by Vendor.

e. *Security Violations*. All systems used by Vendor to provide services must be configured to provide real-time logging of any event that may indicate a system compromise, denial-of-service event, or other security violation. The real-time system logging must immediately notify an administrator when a predetermined event threshold is exceeded. Logs must be reasonably protected from unauthorized access or modification and restricted to only the security administrator or other authorized administrator.

3.5. Log Analysis System. Vendor will use a log analysis, security information, and event management (SIEM) or substantially similar technology to monitor, filter, and log network activity for the purposes of security and intrusion detection. Vendor will use mobile device management (MDM) systems for each of its Personnel's work-related mobile devices.

4. Disaster Recovery and Business Continuity Planning. Vendor shall implement, maintain, and regularly test commercially reasonable disaster recovery and business continuity programs designed to protect the confidentiality and integrity of Opendoor Information during recovery operations. Vendor will ensure these programs do not reduce security in any way. Where Vendor has stored or processed Opendoor Information locally, it shall ensure the availability of such Opendoor Information through the use of backups. All backups must be encrypted and must be stored in a secure location.

5. Data Transfer. Vendor will not permit Opendoor Information to be transferred to any external or removable storage media or any Personnel's personal mobile devices unless (i) there is a pre-approved business need and (ii) such transfer is conducted in accordance with the Security Policy.

6. Data Breach Incident Detection, Notification, and Response.

6.1. Incident Detection. Vendor must implement and maintain both operational incident detection capabilities as well as a comprehensive written incident response plan for responding to suspected or known security incidents or system breaches (the "**Incident Response Plan**"). Such Incident Response Plan must include methods to (i) protect evidence of activity from modification or tampering and (ii) properly allow for the establishment of a chain of custody for evidence.

6.2. Notification. Vendor must notify Opendoor of any unauthorized access, modification, or improper disclosure of Opendoor Information in Vendor's possession or control (a "**Service Data Breach**") without undue delay but within no less than forty-eight (48) hours of Vendor's discovery of the Service Data Breach. Such notification shall include the information

of the relevant point of contact, a preliminary technical analysis of the breach, and the remediation plan Vendor plans to implement within a reasonable timeframe. Vendor shall also, at its sole cost, conduct a more comprehensive security incident investigation without undue delay and provide Opendoor with a comprehensive report detailing how the incident occurred, what information (if any) was disclosed as a result, for how long such information (if any) was disclosed, which person(s) or parties were involved in the Service Data Breach, and the Vendor's remediation activities.

6.3. Response. In the event of confirmed Service Data Breach, Vendor shall comply with any and all of Opendoor's reasonable requests, which may include (without limitation) (i) assisting Opendoor in complying with data breach incident notification requirements under applicable law; (ii) performing, and providing Opendoor with the results of, an independent audit conducted on Vendor's control environment and the controls Vendor has in place with respect to the collection, storage, processing, and use of Opendoor Data; (iii) taking all reasonable steps, as required by applicable law and consistent with industry best practices and standards, to mitigate and correct the effects of any Service Data Breach; and (iv) ceasing or suspending any and all use of Opendoor Information upon receipt of written request from Opendoor. Vendor shall not issue any public communications regarding a Service Data Breach without Opendoor's prior written approval, provided that the foregoing shall not limit or restrict Vendor from communicating with legal authorities, auditors, insurance providers, or legal advisors bound by confidentiality obligations substantially similar to those set forth under the Agreement.

7. Compliance.

7.1. Security Standards. Vendor shall maintain compliance with at least ***one*** of the following: (i) SSAE 18 SOC 2 Type 2 or (ii) ISO 27001 ***OR*** its equivalent standards. Vendor shall provide Opendoor with audit reports or evidence of certification upon request. Vendor will conduct third-party security and penetration tests on applications and infrastructure to identify security vulnerabilities at least once annually. Vendor will provide summary reports of security test reports to Opendoor upon request.

7.2. Audit. Opendoor shall have the right, at its sole expense, to perform an independent audit of Vendor's control environment and the controls Vendor has in place with respect to the collection, storage, processing, and use of Opendoor Information in connection herewith at least once annually. Such audit shall not materially impact or interfere with Vendor's networks, systems, or Vendor's services. Vendor shall provide Opendoor with a copy of any resulting audits report upon request.

7.3 Compliance by Third Parties. Vendor shall require any third parties to whom Vendor delegates some portion of Vendor's services and/or any third-party facilities used in connection with the provision of Vendor's services to adhere to the same or equivalent security standards set forth in this Addendum. Vendor shall conduct vendor risk assessments of all such third party service providers and facilities to ensure that such third parties adhere to the same or equivalent security standards set forth in this Addendum.

8. Survival. This Addendum shall survive the expiration or termination of the Agreement for as long as Opendoor Information Is stored, processed, collected, or used by, or on behalf of Vendor.