DATA PROCESSING ADDENDUM (PARTNERS)

This Data Protection Addendum ("**DPA**" or "**Addendum**")is entered into between AgileBits, Inc. d.b.a. 1Password ("**1Password**") and Manage Service Provider ("**Partner**") (each be referred to herein as a "**Party**" or collectively referred to as the "**Parties**"), sets forth the terms and conditions relating to the privacy, confidentiality, security, and protection of Personal Data (as defined below) that may be made available pursuant to any agreement or order for products or services made between the Parties (the "**Agreement**"). This Addendum has the same effective date as the Agreement ("**Effective Date**").

1. DEFINITIONS

1.1. 1Password Personnel means any employees, agents, consultants, contractors, or similarly situated individuals of 1Password.

1.2. Applicable Data Protection Laws mean applicable 1Password and regulations in the country or region where Personal Data is being Processed, including without limitation the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations ("**CCPA**"), the European General Data Protection Regulation ("**GDPR"**), the UK Data Protection Act 2018 ("**UK GDPR**"), Swiss Federal Act on Data Protection ("**FADP**"), and the Canadian Personal Information Protection and Electronic Documents Act (**PIPEDA**), as each may be amended from time to time.

1.3. Authorized User has the same meaning as defined in the Agreement, or if not such meaning is given means, individuals authorized by the Controller to use the Services, and for whom a subscription to the Services has been purchased through an Order Form. Authorized Users may include, for example, Controller's and its affiliates' employees, consultants, clients, external users, contractors, agents, and third parties with which Controller does business.

1.4. Controller means the party, which alone or jointly determines the purposes and means of the Processing of Personal Data. Controller shall be read to align with the definitions of comparable terms, such as business, under Applicable Data Protection Laws.

1.5. Customer means Managed Customer as defined in the Agreement, or, if not such meaning is given, means the Controller of Personal Data pursuant to any agreement for products or services offered by 1Password, including services offered under 1Password's Partner Agreement.

1.6. Customer Data means Personal Data that 1Password collects, receives, and/or Processes on behalf of and in accordance with the instructions of the Controller or their Processor pursuant to the Agreement, excluding any Personal Data that 1Password Processes as a Controller. Examples of Customer Data include lists of Authorized User names, emails, designated roles or other contact information.

1.7. Data Subject means the identified or identifiable person to whom Personal Data relates.

1.8. De-identified Data means data that cannot reasonably be used to infer information about, or otherwise be linked to, an Authorized User and where such data is Processed only in accordance with the Agreement. It also means Personal Data that is "de-identified" (as the term is defined by the CCPA) when disclosed by one Party to the other.

1.9. Diagnostic Data means Personal Data Processed by 1Password through the provision of its services and that is necessary to the provision of its services, including data regarding Authorized User's customer service interactions and relevant meta data regarding the functionality of the services.

1.10. Information Security Program means technological, physical and administrative safeguards, including without limitation, policies, procedures, guidelines, practices, standards and controls that ensure the confidentiality, security, integrity and availability of Personal Data.
1.11. Personal Data means any information, whether in electronic or paper-based form, which is Processed pursuant to the Agreement and which relates to or could reasonably be related to an identified or identifiable natural person. Personal Data shall be read to align with the definitions of terms such as personal data, personal information, and personally identifiable information under Applicable Data Protection Laws.
1.12. Personal Data Breach means any **(i)** loss or theft of; **(ii)** unauthorized use, disclosure, alteration, acquisition of or access to, or other unauthorized Processing of; or **(iii)** unauthorized access to or use of, inability to access, or malicious infection of Personal Data that reasonably may compromise its privacy or security.
1.13. Process or **Processing** means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collecting, viewing, accessing, storing, organizing, altering, using, disclosing or destroying. Process shall be read to align with comparable terms under Applicable Data Protection Laws.
1.14. Processor means the party, which Processes Personal Data on behalf of the Controller. Processor shall be read to align with the definitions of comparable terms, such as processor or service provider, under Applicable Data Protection Laws.
1.15. Secure Data means Personal Data stored by Authorized Users within the 1Password service offering. Secure data is subject to end-to-end encryption, which can only be decrypted using Authorized User credentials. 1Password does not have the ability to decrypt or otherwise access unencrypted Secure Data.
1.16. Service Data means Personal Data 1Password collects or generates during the provision and administration of the services and related technical support, excluding any Customer Data.
1.17. Sub-Processor means any third-party service provider engaged by 1Password that Processes Personal Data under the instructions or supervision of 1Password.

2. DATA PROCESSING

2.1. Scope and Roles

2.1.1. This DPA applies to the Processing of Personal Data pursuant to the Agreement.
2.1.2. The Parties agree that Partner is the “Business” and 1Password is the “Service Provider” as those terms are defined by the CCPA.
2.1.3. With regard to Customer Data and Secure Data, Partner is the Controller or authorized Processor of the Controller, and 1Password is the Processor.
2.1.4. With regard to Diagnostic Data and Service Data, 1Password is a Controller.
2.1.5. 1Password will Process Diagnostic Data and Service Data for the following purposes: **(i)** to carry out core business functions such as accounting, billing, and filing taxes; **(ii)** to provide and improve the Services; **(iii)** to manage the Partner relationship, including communicating with Partner, Customer, and designated Authorized Users in accordance with their account preferences; **(iv)** to secure the Services, including fraud prevention, performance monitoring, business continuity and disaster recovery; and **(v)** to comply with 1Password’s legal obligations.

2.2. Instructions, Subject Matter, and Nature of Processing

2.2.1. 1Password will Process Customer Data and Secure Data only for the business purposes specified in the written instructions contained in the Agreement, this DPA, or as reasonably specified through Partner’s use of the Services Admin settings, or as otherwise instructed by the relevant Controller in writing, including email.

2.2.2. If Partner acts as a Processor under the instructions of the relevant Customer and Controller of Personal Data, Partner warrants that the Processing instructions as set out in the Agreement and this DPA, including its authorizations to 1Password for the appointment of Subprocessors in accordance with this DPA, have been authorized by the relevant Controller. 1Password acknowledges and accepts that the commitments contained in this DPA are for the benefit of the ultimate Controller.

2.2.3. Partner will forward to the relevant Customer and Controller promptly and without undue delay any notifications provided to Partner by 1Password under this DPA.

2.2.4. Partner represents that it takes commercially reasonable steps to comply with Applicable Data Protection Laws, that it has a valid lawful basis for Processing Personal Information, and that it will not knowingly instruct 1Password to process Personal Data in a manner that violates any Applicable Data Protection Laws. 1Password will promptly inform Partner if, in 1Password's opinion, an instruction infringes on any Applicable Data Protection Laws.

2.3. CCPA. The definitions "**Sale**", "**Sell**", "**Share**", and "**Business Purpose**" as used in this Addendum have the meaning given to them under the CCPA. 1Password will not: **(i)** Sell or Share Personal Data; **(ii)** retain, use, or disclose Personal Data for any purpose other than described under Section 2.2.1 of this Addendum or otherwise permitted by the CCPA; or (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Customer and 1Password, unless permitted by the CCPA.

3. DATA PROCESSING OBLIGATIONS

3.1. Confidentiality of Personal Data

3.1.1. 1Password will maintain the confidentiality of Personal Data processed pursuant to the Agreement and this Addendum. Secure Data shall remain encrypted and will not be stored in a manner that renders it accessible to 1Password without the specific authorization and access credentials of the relevant Authorized User.

3.1.2. 1Password will take commercially reasonable efforts to ensure that 1Password Personnel are only granted access to Personal Data on a need-to-know basis. 1Password will ensure that 1Password Personnel with access to Personal Data have received adequate training as to the proper handling of Personal Data under Applicable Data Protection Laws. 1Password will ensure that 1Password Personnel with access to Personal Data are subject to an enforceable contractual or statutory confidentiality obligation regarding such Personal Data.

3.1.3. 1Password will not retain, use, disclose, or otherwise Process Personal Data for any purposes other than those specified in the Agreement, this DPA, or as otherwise permitted by law.

3.1.4. 1Password will not combine, as the term is used under the CCPA, Service Data, Diagnostic Data, or Secure Data with other personal data it collects from other entities or on its own behalf unless permitted by Applicable Data Protection Laws.

3.2. Sub-Processors

3.2.1. Partner authorizes 1Password to engage Sub-Processors as identified in Schedule C and under "List of SubProcessors" at: https://1password.com/legal-center/ as which may be amended from time to time.

3.2.2. Partner generally authorizes 1Password to engage additional Sub-Processors as needed from time to time in accordance with the following conditions: (i) No Sub-Processors will, under any circumstances, have access to Secure Data in an unencrypted format; (ii) the Sub-Processor will process Personal Data only in accordance with the Agreement and if required under Applicable Data Protection Laws, the obligations described under this DPA are imposed on the Sub-Processor; and (iii) Prior to

engaging a new Sub-Processor to Process Personal Data under this DPA, Partner may object to 1Password's use of a new Sub-Processor by notifying 1Password within 30 days of receiving notice of engagement with a potential new Sub-Processor. In the event of an objection notice, the Parties agree to take commercially reasonable efforts to identify and remediate relevant issues with the identified Sub-Processor.

3.2.3. 1Password will not disclose Personal Data to a Sub-Processor unless 1Password has entered into a written contract with the Sub-Processor that provides no less protection for Personal Data as is provided under the Agreement and this Addendum.

3.2.4. For the purposes of the CCPA, 1Password and Partner acknowledge and agree that 1Password will not "Sale" Personal Data or "Share" Personal Data without an applicable Business Purpose to its authorized Sub-Processors when providing its Services under the Agreement.

3.3. Compliance with Privacy and Information Security Requirements

3.3.1. 1Password's Processing of Personal Data will comply with Applicable Data Protection Laws. Each Party will comply with the requirements set forth under the CCPA with regard to processing of De-identified Data.

3.3.2. 1Password will implement an appropriate Information Security Program that is consistent with Applicable Data Protection Laws and industry standards, and that is reasonable in light of the nature of the data being Processed. 1Password will maintain reasonable administrative, physical, and technical safeguards that are necessary to ensure the security, confidentiality, and integrity of Personal Data under the Agreement, these measures are detailed in Schedule B.

3.3.3. Partner without prejudice to 1Password's obligations under this DPA, and anywhere else in the Agreement, as between 1Password and Partner, Partner is responsible for its and it's Managed Customer's use of the Services, including the processing of any copies of Personal Data outside of 1Password or its Sub-Processors systems, including securing the account authentication credentials, systems and devices Partner and its Managed Customers use to access the Services.

3.3.4. In the event that 1Password determines that it can no longer meet its obligations under this Addendum or Applicable Data Protection Laws, 1Password agrees to cease processing Personal Data under the Agreement and notify the Partner in writing of such determination without undue delay.

3.4. Personal Data Breach Response

3.4.1. 1Password shall notify Partner without undue delay, and in any event within forty-eight (48) hours, in the event of a Personal Data Breach. Such notice will summarize the impact on applicable data as well as any corrective actions taken or to be taken by 1Password.

3.4.2. 1Password will promptly respond to and investigate any Personal Data Breach in a commercially reasonable manner that complies with Applicable Data Protection Laws. 1Password agrees to provide Partner with all information reasonably necessary to comply with Applicable Data Protection Laws and assist in commercially reasonable remediation efforts.

3.4.3. 1Password's obligation to report or respond to a Personal Data Breach under this Section is not an acknowledgement by 1Password of any fault or liability with respect to the Personal Data Breach.

3.5. Cooperation and Information Requests

3.5.1. 1Password will in a manner consistent with the functionality of the Services enable Partner or the relevant Customer and Controller to respond to requests by Authorized Users regarding their Personal Data ("**Data Subject Rights Request**"). If 1Password receives a Data Subject Rights Request from a Data Subject that relates to Partner's use of the Services and identifies Partner, 1Password will advise the Data

Subject to submit their request to Partner and notify Partner without delay of any Data Subject Rights Request received by 1Password pursuant to Applicable Data Protection Laws with which the relevant Controller must comply. Partner or the relevant Controller will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

3.5.2. 1Password will provide reasonable assistance to Partner (or where Partner is a Processor, to the relevant Controller) with any data protection impact assessments ("**DPIA**"), prior consultations with data protection supervisory authorities, and privacy by design procedures in accordance with Applicable Data Protection Laws.

3.5.3. 1Password will reasonably cooperate with Partner, in the course of any investigation of, or claim against, the relevant Controller relating to the Processing of Personal Data.

3.5.4. 1Password will notify Partner without delay of any Data Subject Rights Request received by 1Password pursuant to Applicable Data Protection Laws with which the relevant Controller must comply.

3.5.5. Third Party Requests. Unless prohibited by law, 1Password will promptly notify Partner of any valid, enforceable subpoena, warrant, or court order from law enforcement or public authorities compelling 1Password to disclose Personal Data under Partner's or the relevant Customer and Controller. 1Password will follow its published law enforcement policies in responding to such requests. In the event that 1Password receives an inquiry or a request for information from any other third party (such as a regulator or data subject) concerning the Processing of Personal Data under Customer's control, 1Password will redirect such inquiries to Partner, and will not provide any information unless required to do so under applicable Law.

4. TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

The European Commission ("**EC**"), pursuant to Article 45 of Regulation 2016/679, the United Kingdom Information Commissioner's Office ("**ICO**"), and the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**"), have issued adequacy decisions in respect of Canadian commercial organizations. As a result of these decisions, the transfer of Personal Data to Canada, in connection with the Agreement, is subject to an adequate level of protection, in compliance with Applicable Data Protection Laws, and Customer agrees that no additional transfer mechanism is required for transfers of Personal Data to Canada. In the event that the EC, UK ICO, and/or FDPIC no longer recognize Canada as an "adequate" jurisdiction for data transfers; in the event that the Services change to result in a direct transfer of Personal Data to jurisdictions outside of Canada that do not maintain an adequacy determination; or if Customer determines that the transfer comprises Personal Data that requires a Data Transfer Mechanism (as defined in ANNEX I, the Data Transfers Schedule, which is incorporated into this DPA as ANNEX I, will apply.

5. AUDIT AND DEMONSTRATION OF COMPLIANCE

1Password shall make available to Customer, pursuant to Customer's reasonable written request, all information reasonably necessary for Customer to demonstrate compliance with Applicable Data Protection Laws regarding 1Password's Processing of Personal Data under the Agreement by first providing (on a confidential basis) a summary copy of its ISO 27001 certification, SOC 2 Type 2 report, or any other applicable certification. If more information is required or if 1Password is required under Applicable Data Protection Laws, the Partner may request an audit. 1Password will assist and cooperate with Partner or an independent auditor appointed by Partner to audit 1Password's compliance with its obligations under this DPA. Partner and 1Password will discuss

and agree in advance on the audit scope and duration. 1Password may charge a fee based on its reasonable costs for audits conducted at Partner's request.

6. RETURN OR DELETION OF PERSONAL DATA

On termination or expiration of the Agreement, 1Password shall promptly return or delete all Customer Data and Secure Data Processed pursuant to the Agreement upon Partner's reasonable request; provided, that 1Password shall have the right to retain a copy of any such Personal Data to the extent required by law.

7. MISCELLANEOUS

7.1. This DPA supersedes and replaces all prior representations, understandings, communications, and agreements by and between the parties in relation to the Secure Data and Customer Data and the matters set forth in this DPA. In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) will prevail: (a) the Standard Contractual Clauses if applicable; then (b) this DPA; and then (c) the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply.
7.2. Each Party's liability arising out of or in connection with this Addendum and its subject matter shall be subject to the limitations of liability set forth in the Agreement.
7.3. This Addendum supplements the Agreement with respect to any Processing of Personal Data pursuant to the Agreement. In the event of any conflict between this Addendum and the Agreement, the terms of this Addendum shall prevail as to the matters at issue herein.
7.4. Each Party's compliance with this Addendum, and any actions required of each respective Party herein, shall be at that Party's sole and exclusive expense.

ANNEX I– DATA TRANSFERS ADDENDUM

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the DPA or Agreement.

1. DEFINITIONS

For the purposes of this Schedule, the following definitions apply:

- **Data Transfer Mechanism** means a transfer mechanism that enables the lawful cross-border transfer of Personal Data under Applicable Data Protection Laws, which includes transfer mechanisms that are required under Applicable Data Protection Laws in the EEA, Switzerland, and the UK, such as the EEA SCCs, the UK International Data Transfer Addendum and any data transfer mechanism available under Applicable Data Protection Laws that is incorporated into this DPA.
- **EEA** means the European Economic Area.
- **EEA SCCs** means the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to the GDPR.
- **Restricted Transfer** means **(i)** where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; **(ii)** where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; or **(iii)** where the Swiss FADP applies, a transfer of Personal Data from Switzerland to any other country that does not provide appropriate levels of protection under Article 16, Paragraph 1 of the FADP.
- **UK International Data Transfer Addendum** means the international data transfer addendum to the EEA SCCs issued by the United Kingdom's Information Commissioner's Office.

2. ORDER OF PRECEDENCE

If, in connection with 1Password's providing the Services to Customer, more than one Data Transfer Mechanism could apply to a transfer of Personal Data, Customer and 1Password agree that the transfer will be subject to one Data Transfer Mechanism only, according to the following order of precedence:

(a) the EEA SCCs;
(b) the UK International Data Transfer Addendum; and
(c) any other data transfer mechanism available under Applicable Data Protection Laws that is incorporated into this DPA.

3. TRANSFERS FROM THE EEA

Where a Restricted Transfer is made from the EEA, the EEA SCCs are incorporated into this DPA and apply to the transfer as follows:

(a) with respect to Restricted Transfers from Customer to 1Password, Module One applies where both 1Password and Customer are Controllers, and Module Two applies where Customer is a Controller and 1Password is a Processor; Module Three applies where Partner is a Processor and 1Password is a Processor;
(b) in Clause 7, the optional docking clause does not apply;

(c) in Clause 9(a) of Module Two, Option 2 applies, and the time period for prior notice of Subprocessor changes is 30 days;
(d) in Clause 11(a), the optional language does not apply;
(e) in Clause 17, Option 1 applies with the governing law being that of Ireland;
(f) in Clause 18(b), disputes will be resolved before the courts in Dublin, Ireland;
(g) Annex I of the EEA SCCs is completed with the information in Schedule A to this Annex;
(h) Annex II of the EEA SCCs is completed with the information in Schedule B to this Annex; and
(i) Annex III of the EEA SCCs is completed with the information in Schedule C to this Annex.

4. TRANSFERS FROM THE UK

Where a Restricted Transfer is made from the UK, the UK Transfer Addendum is incorporated into this DPA and applies to the transfer as follows: the UK Transfer Addendum is completed with the information in Section 3.4.2 and Schedules A, B, and C to this Annex; and both "Importer" and "Exporter" are selected in Table 4.

5. TRANSFERS FROM SWITZERLAND

Where a Restricted Transfer is made from Switzerland, the Parties enter into the EEA SCCs as described under section 3.4.2 above. With regard to the EEA SCCs, the parties agree that:
(a) references to provisions of the GDPR are to be understood as references to the corresponding provisions of the FADP;
(b) the term 'Member State' also applies to Switzerland;
(c) the competent authorities under Clause 13, and in Annex I(C) include the Swiss Federal Data Protection and Information Commissioner;
(d) the governing jurisdiction for claims under the FADP is that of Switzerland; and
(e) any dispute arising from these clauses under the FADP shall be resolved by the courts of Zurich, Switzerland.

SCHEDULE A

This Schedule A to Annex I includes certain details of the Processing of Personal Data as required by Article 28(3) GDPR.

A. LIST OF PARTIES

Data exporter

Name: The Party to the Agreement with 1Password

Address: As specified in the Agreement.

Contact person's name, position and contact details: The address, name and details associated with Customer's 1Password account or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: Providing access to 1Password services to internal personnel.

Signature and date: By using the Services to transfer Personal Data to the data importer, the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller or Processor with respect to Customer Data and Secure Data

Data importer

Name: AgileBits Inc. dba 1Password

Address: 4711 Yonge Street, 10th Floor, Toronto, ON, M2N 6K8 Canada

Contact person's name, position and contact details: Data Privacy Officer, privacy@agilebits.com with a copy to legal@agilebits.com

Activities relevant to the data transferred under these Clauses: Providing access to 1Password Services to Partner and Authorized Users.

Signature and date: The data importer will be deemed to have signed this Annex I on the transfer of Personal Data by the data exporter in connection with the Services.

Role (controller/processor): Processor with respect to Customer Data and Secure Data.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The Customer Data transferred concern individuals about whom Customer Data is provided to 1Password via the Services by (or at the direction of) Partner or Authorized Users. This may include, but is not limited to, Customer Data relating to Partner's Managed Customers and the Managed Customer's employees.

Categories of personal data transferred

Customer Data as defined in the Addendum. No special categories, only data that are provided by the data subjects for the purpose of setting up the account and customer support.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
No sensitive data is transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Continuous basis.

Nature of the processing
1Password is a Processor and provides its proprietary services, which Partner, Customer and Authorized Users can use to store data in any format behind a master password protected vault. Such master password is created, protected and preserved by Partner or Customer's Authorized Users only, and 1Password or its agents at no time have access, knowledge or ability to know the master password. All data stored or preserved behind the master password protected vault remains encrypted at all times (during transit and at rest) and is hosted via cloud-based data servers.

Purpose(s) of the data transfer and further processing
To provide services under the Agreement and to secure, monitor, and improve the Services in accordance with the Addendum

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
For the duration of the contract between the Partner and 1Password except for any archive data required to be maintained under the laws or unless otherwise agreed between Controller and 1Password.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
The subject matter and nature of the Processing by Sub-processors are as specified in Section 3.2 of the Addendum. The duration of the Processing carried out by the Sub-processors will be for the duration of the Agreement between the Partner and 1Password and thirty (30) days following the termination or expiration of the Agreement unless otherwise agreed.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be determined in accordance with the applicable Data Protection Laws.

SCHEDULE B

1PASSWORD TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1Password will maintain an information security program designed to (a) secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the 1Password Services, and (c) minimize physical and logical security risks to the 1Password Services, including through regular risk assessment and testing. 1Password will designate one or more employees to coordinate and be accountable for the information security program. Capitalized terms not otherwise defined in this document have the meanings assigned to them in the DPA or Agreement. 1Password's information security program will include the following measures:

1. LOGICAL SECURITY

1.1 Access Controls. 1Password will make the Services accessible only to authorized personnel, and only as necessary to maintain and provide the Services. 1Password will maintain access controls and policies to manage authorizations for access to the 1Password Services from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. 1Password will maintain access controls designed to restrict unauthorized access to data and segregate each customer's data from other customers' data.

1.2 Restricted User Access. 1Password will **(i)** provision and restrict user access to the Services in accordance with least privilege principles based on personnel job functions; **(ii)** require review and approval prior to provisioning access to the Services above least privileged principles, including administrator accounts; **(iii)** require at least quarterly review of Services access privileges and, where necessary, revoke Services access privileges in a timely manner; and **(iv)** require two- factor authentication for access to the Services from remote locations.

1.3 Vulnerability Assessments. 1Password will perform regular external vulnerability assessments and penetration testing of the Services, and will investigate identified issues and track them to resolution in a timely manner.

1.4 Application Security. Before publicly launching new Services or significant new features of Services, 1Password will perform application security reviews designed to identify, mitigate and remediate security risks.

1.5 Change Management. 1Password will maintain controls designed to log, authorize, test, approve and document changes to existing Services resources, and will document change details within its change management or deployment tools. 1Password will test changes according to its change management standards prior to migration to production. 1Password will maintain processes designed to detect unauthorized changes to the Services and track identified issues to a resolution.

1.6 Data Integrity. 1Password will maintain controls designed to provide data integrity during transmission, storage and processing within the Services. 1Password will provide Customer the ability to delete Customer Data from the Services.

1.7 Business Continuity and Disaster Recovery. 1Password will maintain a formal risk management program designed to support the continuity of its critical business functions ("**Business Continuity Program**"). The Business Continuity Program includes processes and procedures for the identification of, response to, and recovery from, events that could prevent or materially impair 1Password's provision of the Services (a "**BCP Event**"). The Business Continuity Program includes a three-phased approach that 1Password will follow to manage BCP Events:

(i) *Activation & Notification Phase.* As 1Password identifies issues likely to result in a BCP Event, 1Password will escalate, validate and investigate those issues. During this phase, 1Password will analyze the root cause of the BCP Event.

(ii) *Recovery Phase.* 1Password assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.

(iii) *Reconstitution Phase.* 1Password leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services have been restored. Following such confirmation, 1Password conducts a post-mortem analysis of the BCP Event.

1.8 Incident Management. 1Password will maintain corrective action plans and incident response plans to respond to potential security threats to the Services. 1Password incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The 1Password incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation.

1.9 Storage Media Decommissioning. 1Password will maintain a media decommissioning process that is conducted prior to the final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry-standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.

2. PHYSICAL SECURITY

2.1 Access Controls. Where applicable, 1Password will **(i)** implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the 1Password Services, **(ii)** use appropriate control devices to restrict physical access to the 1Password Services to only authorized personnel who have a legitimate business need for such access, **(iii)** monitor physical access to the 1Password Services using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, **(iv)** log and regularly audit physical access to the 1Password Services, and **(v)** perform periodic reviews to validate adherence with these standards.

2.2 Availability. 1Password will **(i)** implement redundant systems for the 1Password Services designed to minimize the effect of a malfunction on the 1Password Services, **(ii)** design the 1Password Services to anticipate and tolerate hardware failures, and **(iii)** implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

3. 1PASSWORD EMPLOYEES

3.1 Employee Security Training. 1Password will implement and maintain employee security training programs regarding 1Password information security requirements. The security awareness training programs will be reviewed and updated at least annually.

3.2 Background Checks. Where permitted by law, and to the extent available from applicable governmental authorities, 1Password will require that each employee undergo a background investigation that is reasonable and appropriate for that employee's position and level of access to the 1Password Services.

3.3 Continued Evaluation. 1Password will conduct periodic reviews of the information security program for the 1Password Services. 1Password will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.

SCHEDULE C

SUB-PROCESSORS LIST

For the most up-to-date list of our Sub-Processors, please review the documentation located at https://1passwordstatic.com/files/legal-center/notice-of-updates-to-the-1password-subprocessor-list.pdf.