DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") supplements the Terms of Use ("Terms") and/or other written or electronic agreement ("**Agreement**") between: (i) Keeper Security, Inc. **("Keeper" or "Vendor")** acting on its own behalf and as agent for any Keeper Affiliate; and (ii) _____ ("**Customer**") acting on its own behalf and as agent for any Customer Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement, or is undefined in either the Addendum or Agreement, such terms shall have the meaning as per the European General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)(as amended from time to time)("GDPR"). Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions

In this Addendum, the following terms shall have the meanings set out below:

1.1. **Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. **Applicable Laws** means all laws applicable to the Processing of Customer Data, which may include EU Data Protection Laws, other laws of the European Union or any Member State thereof, and the laws of any other country to which the Customer or the Customer Data is subject.

1.3. **Controller** means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

1.4. **Data Subject** refers to a natural person whose Personal Data is processed in the context of this Addendum.

1.5. **EU Data Protection Laws** means GDPR and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislation, if any.

1.6. **GDPR** means EU General Data Protection Regulation 2016/679;

1.7. **Personal Data** means any information relating to an identified or identifiable natural person.

1.8. **Processor** means the entity that processes Personal Data on behalf of a Controller.

1.9. **Processing or Process** means any operation or set of operations which is performed on Personal Data, individually or in sets, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

1.10. **Services** means the services and other activities to be supplied or carried out by Keeper for Customer pursuant to the Agreement;

1.11. **Standard Contractual Clauses** means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection set out in the European Commission's decision 2021/914 of 4 June 2021, as attached hereto as Sub-Appendix C.

1.12. **Sub-Processor** means any Processor engaged by Keeper Security to process personal data in connection with the Services.

2. PROCESSING OF PERSONAL DATA

2.1. The purpose of the processing under the Addendum is the provision of the Services by Keeper as specified in the Agreement. The parties agree that with regard to the processing by Keeper on behalf of Customer, Customer is the Controller and Keeper is the Processor. The categories and types of Personal Data processed by Keeper are listed in Sub-Appendix A.

2.2. Keeper may only act and process the Personal Data in accordance with the documented instructions from the Customer (the "Instruction"), unless required by law to act without such instruction. The Instruction at the time of entering into this Addendum is that Keeper may only process the Personal Data with the purpose of delivering the Services as described in the Agreement. Subject to the terms of this Addendum, and with mutual agreement of the parties, the Customer may issue additional written instructions consistent with the terms of this Addendum. The Customer is responsible for ensuring that all individuals who provide written instructions are authorized to do so.

2.3. Keeper will inform the Customer of any instruction that it deems to be in violation of Applicable Laws, including EU Data Protection Laws, and will not execute the instructions until they have been confirmed or modified.

3. CONFIDENTIALITY AND SECURITY

3.1. Keeper shall treat all Personal Data as strictly confidential information. The Personal Data may not be copied, transferred or otherwise processed in conflict with the Instruction, unless the Customer in writing has agreed. Keeper's employees shall be subject to an obligation of confidentiality that ensures that the employees shall treat all the Personal Data under this Addendum with strict confidentiality. Personal Data will only be made available to personnel that require access to such Personal Data for the delivery of the Services and this Addendum.

3.2. Keeper shall implement the appropriate technical and organizational measures as set out in this Agreement and in the Applicable Laws, including in accordance with GDPR, article 32. The security measures are subject to technical progress and development. Keeper may update or modify the security measures from time-to-time provided that such updates and modifications do not result in the degradation of the overall security. Keeper's Information Security Policy is available in Sub-Appendix D.

4. RIGHTS OF THE DATA SUBJECT

4.1. If the Customer receives a request from a data subject for the exercise of the data subject's rights under the Applicable Laws and the correct and legitimate reply to such a request requires Keeper's assistance, Keeper shall assist the Customer by providing the necessary information and documentation. Keeper shall be given reasonable time to assist the Customer with such requests in accordance with the Applicable Laws.

4.2. If Keeper receives a request from a data subject for the exercise of the data subject's rights under the Applicable Laws and such request is related to the Personal Data of the Customer, unless prohibited by law, Keeper will immediately forward the request to the Customer and refrain from responding to the person directly unless and until otherwise instructed by Customer.

5. PERSONAL DATA BREACHES

5.1. Keeper shall give immediate notice to the Customer if a breach occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, Personal Data transmitted, stored or otherwise processed on behalf of the Customer (a "Personal Data Breach").

5.2. Keeper shall make reasonable efforts to identify the cause of such a breach and take those step as they deem necessary to establish the cause, and to prevent such a breach from reoccurring.

6. DOCUMENTATION OF COMPLIANCE AND AUDIT RIGHTS

6.1. Upon request by a Customer, for cause or to the extent required by Article 28 of the GDPR, Keeper shall make available to the Customer all relevant information necessary to demonstrate compliance with this Addendum, and shall allow for and reasonably cooperate with audits, including inspections by the Customer or an auditor mandated by the Customer. The Customer shall give notice of any audit or document inspection to be conducted and shall make reasonable endeavours to avoid causing damage or disruption to Keeper's premises, equipment and business in the course of such an audit or inspection. Any audit or document inspection shall be carried out with reasonable prior written notice of no less than sixty (60) calendar days, and shall not be conducted more than once a year.

6.2. The Customer may be requested to sign a non-disclosure agreement reasonably acceptable to Keeper before being furnished with the above.

7. DATA TRANSFERS

7.1. If the parties transfer Personal Data originating from the European Economic Area ("EEA") to a party located in countries outside the EEA that have not received a binding adequacy decision by the European Commission, such transfers shall be made in compliance with applicable data transfer legal requirements and only by documented instructions from Customer.

7.2. If Customer believes these measures are insufficient to satisfy legal requirements under any particular circumstance, Customer shall provide written notice of its grounds for such opinions to Keeper and the Parties shall work together in good faith to find a mutually agreeable alternative.

8. SUB-PROCESSORS

8.1. Keeper is given general authorization to engage third-parties to process the Personal Data ("Sub-Processors") without obtaining any further written, specific authorization from the Customer. Keeper shall complete a written sub-processor agreement with any Sub-Processor. Such an agreement shall at a minimum provide the same data protection obligations as the ones applicable to Keeper, including the obligations under this Addendum. Keeper shall, on an ongoing basis, monitor and control its Sub-Processors' compliance with the applicable Data Protection Law, and documentation of such monitoring and control shall be provided to the Customer, if requested in writing.

8.2. If Sub-Processor performs the agreed services outside the EU/EEA, the Keeper shall ensure their admissibility under data protection law by taking appropriate measures.

8.3. At the time of entering into this Agreement, Keeper is using the Sub-Processors listed in sub-appendix B. Keeper shall notify Customer of any new Sub-Processors, which notice may be given by posting details of such addition to the sub-processors list available at https://www.keepersecurity.com/GDPR.html or by e-mail (where Customer has requested to receive notice by sending an email to gdpr@keepersecurity.com within ten (10) days of executing this Addendum) no less than ten (10) business days before authorizing such Sub-Processor to Process Personal Data in connection with the provision of the Services.

8.4. Customer may, in good faith, reasonably object to Keeper's use of a new Sub-Processor by providing written notice to Processor by e-mail at gdpr@keepersecurity.com within ten (10) business days of receiving notification from Customer of a potential new Sub-Processor. Such written notice shall include, at a minimum, Customer's good faith, reasonable grounds for the objection. Keeper shall use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's use of the Services to avoid processing of Personal Data by the challenged Sub-Processor. The absence of any objections from the Customer within ten (10) business days shall be deemed consent to the relevant Sub-Processor.

8.5. In the event the Customer objects to a new Sub-Processor and Keeper cannot accommodate the Customer's objection, the Customer may terminate the Services with respect only to the Services that cannot be provided by Keeper without the use of the challenged new Sub-Processors by providing written notice to Keeper.

8.6. Keeper is accountable to the Customer for any Sub-Processor in the same way as for its own actions and omissions.

9. TERMINATION; RETURN OR DELETION OF PERSONAL DATA

9.1. Following expiration or termination of the Agreement, Keeper will delete or return to the Customer all Personal Data in its possession as provided in the Agreement except to the extent Keeper is required by the Applicable Laws to retain some or all of the Personal Data (in which case Keeper will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this Addendum will continue to apply to such Personal Data.

10. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

10.1. If Keeper's assistance is necessary and relevant, the parties will cooperate to the extent reasonably necessary in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36. The parties will each bear their respective costs when fulfilling such obligations.

11. MISCELLANEOUS

11.1. **Modification of Addendum:** This Addendum may only be modified by a written amendment signed by each of the Parties.

11.2. **Governing Law:** This Addendum is governed by, and shall be construed in accordance with, the laws governing the Agreement.

11.3. **Invalidity and Severability; Conflict:** If any provision of this Addendum is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this Addendum and all provisions not affected by such invalidity or unenforceability will remain in full force and effect. In the event of any inconsistency between this Addendum and Standard Contractual Clauses entered into by the parties, if any, the Standard Contractual Clauses shall prevail.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed as of the Effective Date.

Keeper Security, Inc.	**Customer**
By: _____ (Authorized Signature)	By: _____ (Authorized Signature)
Name: _____ (Print or Type)	Name: _____ (Print or Type)
Title: _____	Title: _____

SUB-APPENDIX A

1. Personal Data

1.1 Keeper processes the following types of Personal Data in connection with its delivery of the services:

1.1.1 The personal data transferred concern contact information (name, address, email, phone), entity data, navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent or received by end users via the Services.

1.1.2 Information as described in Keeper's Privacy Policy located at https://keepersecurity.com/privacy.

2. Categories of Data Subjects

2.1 Keeper processes personal data about the following categories of data subjects on behalf of the Customer:

2.1.1 Customer

2.1.2 Customer's Authorized End Users, including employees of Customer.

SUB-APPENDIX B – Approved Sub-processors

1.1 The following Sub-Processors shall be considered approved by the Customer at the time of entering into this Agreement. The Parties agree that there is no contemplated transfer of personal data from the EU to countries outside of the EU.

Name	Location	Nature of Processing
Google, Inc.	US	Provision of E-mail delivery services
Google Analytics	US	Usage and website analytics
Salesforce	US	Customer account management
Hubspot	US	Inbound marketing and sales
HelpScout	US	Email support
Hotjar	EU	Website tracking and analytics
Amazon AWS	US/EU	Cloud Infrastructure
Salesloft	US	Data Enrichment
Stripe	US/EU	Payment processor
Atlassian	US	Product Management
PayPal	US	Payment processor
Rakuten	US	Affiliates
Olark	US	Support chat services
Drift	US	Marketing and support chat services
Adjust	Germany	Data Enrichment/Analytics
ZoomInfo	US	Data Enrichment
Impact Tech	US	Data Enrichment
Calendly	US	Account scheduling
ChurnZero	US/EU	Data Enrichment
Braze	US/EU	User communication and marketing
Facebook	US	Social Media
Vimeo	US	Website video display
Survey Monkey	US	Survey analytics
ConnectAndSell	US	Customer account management enrichment

SUB-APPENDIX C

(EU Standard Contractual Clauses)

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:

Address:

Tel.: fax: e-mail:

Other information needed to identify the organisation:
……
(the data **exporter)**

And

Name of the data importing organisation: Keeper Security, Inc.

Address: 820 W. Jackson Blvd., Suite 400, Chicago, IL 60607

Tel.: +1 312-561-3054 fax: N/A e-mail: support@keepersecurity.com

Other information needed to identify the organisation: Not applicable
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Sub-Appendix A.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature

On behalf of the data importer:

Name (written out in full):

Position:

Address Keeper Security, Inc., 820 W. Jackson Blvd., Suite 400, Chicago, IL 60607

Other information necessary in order for the contract to be binding (if any):

Signature

Clause 1

Purpose and scope

(a)The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b)The Parties:

(i)the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I (hereinafter each 'data exporter'), and

(ii)the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I

(d)The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a)These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module Two: Clause 12(a), (d) and (f)

(v) Clause 15.1(c), (d), and (e);

(vi) Clause 16(e);

(vii) Clause 18 – Clause 18 (a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679

Clause 4

Interpretation

(a)Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.

Clause 7 – Optional

Docking clause

(a)An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I

(b)Once it has completed the Appendix and signed Annex I, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.

(c)The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent

possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including

measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

MODULE TWO: Transfer controller to processor

a) SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 4 weeks prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Sub-Appendix B. The Parties shall keep Sub-Appendix up to date.
b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws

Clause 12

Liability

MODULE TWO: Transfer controller to processor

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I, shall act as competent supervisory authority.
b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
    ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
    iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data

exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request

if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i)the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these

Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

MODULE TWO: Transfer controller to processor

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b) The Parties agree that those shall be the courts of Ireland (specify Member State).
c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I to the Standard Contractual Clauses

Data exporter

The data exporter is the Customer, as defined in the Agreement.

Data importer

The data importer is Keeper Security, Inc., a global provider of SaaS zero-knowledge encryption products and services.

Data subjects

The personal data transferred concerns the data exporter and data exporter's Authorized End Users including employees, contractors and the personnel of customers, suppliers, collaborators, and subcontractors.

Categories of data

The personal data transferred concerns contact information (name, address, email, phone), entity data, navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent or received by Authorized End Users via the Services.

Special categories of data (if appropriate)

The parties do not anticipate the transfer of special categories of data.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Scope of Processing

Personal data may be processed for the following purposes: (a) to provide the Services (which may include the detection, prevention, and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the Agreement.

The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its sub-processors maintain facilities as necessary for it to provide the Services.

Term of Data Processing

Data processing will be for the term specified in the Agreement. For the term of the Agreement, and for a reasonable period of time after the expiry or termination of the Agreement, the Data Importer will provide Data Exporter with access to, and the ability to export, the Data Exporter's personal data processed pursuant to the Agreement.

Data Deletion

For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to delete data as detailed in the Agreement.

Access to Data

For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to correct, block, export and delete the Data Exporter's personal data from the Services in accordance with the Agreement.

Sub-processors

The Data Importer may engage sub-processors to provide parts of the Services. The Data Importer will ensure sub-processors only access and use the Data Exporter's personal data to provide the Data Importer's products and services and not for any other purpose.

DATA EXPORTER:

Name:

Authorised Signature

DATA IMPORTER: Keeper Security, Inc.

Name:

Authorised Signature:

Annex II TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer

Keeper Security will maintain the administrative, physical and technical safeguards in place set forth a in Sub-Appendix D. Notwithstanding any provision to the contrary otherwise agreed to by Data Exporter, Keeper Security may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

DATA EXPORTER:

Name:

Authorised Signature

DATA IMPORTER: Keeper Security, Inc.

Name:

Authorised Signature:

SUB-APPENDIX D
Keeper Security, Inc.
Security Disclosure

Keeper Security, Inc. (KSI) is passionate about protecting its customer's information with Keeper mobile and desktop security software. Millions of consumers and businesses trust Keeper to secure and access their passwords and private information.

Keeper's software is constantly improved and updated to provide our customers with the latest in technology and protection. This page provides an overview of Keeper's security architecture, encryption methodologies and hosting environment as of the current published version. An overview into the technical details involving our encryption and security methods are described in this document.

Data Protection
Zero-trust begins with password security. KSI creates its products using a zero-trust security framework that is based on not trusting any user within the architecture. Zero-trust assumes that all users and devices could potentially be compromised and thus, each user must be verified and authenticated before they can access a website, application or system. This cybersecurity framework underpins Keeper's cybersecurity platform. The platform provides IT administrators full visibility into all users, systems and devices they are accessing which helps ensure compliance with industry and regulatory mandates. In order to have a zero-trust framework in an organisation, it must have world-class password security that is supported with a zero-knowledge security architecture.

KSI is a **Zero-Knowledge** security provider. The Keeper user is the only person that has full control over the encryption and decryption of their data. With Keeper, encryption and decryption occurs only on the user's device upon logging into the vault. Each individual record stored in the user's vault is encrypted with a random 256-bit AES key that is generated on the user's device. The record keys are protected by an additional key, called the Data Key. The Data Key is encrypted by a key derived on the device from the user's Master Password. Data stored at rest on the user's device is also encrypted by another key, called the Client Key. Secure record syncing between the user's devices is also encrypted at the network layer and routed through Keeper's Cloud Security Vault. This multi-tiered encryption model provides the most advanced data protection available in the industry.

The encryption key that is needed to decrypt the data always resides with the Keeper user. KSI cannot decrypt the user's stored data. KSI does not have access to a customer's master password nor does KSI have access to the records stored within the Keeper vault. KSI cannot remotely access a customer's device nor can it decrypt the customer's vault. The only information that Keeper Security has access to is a user's email address, device type and subscription plan details (e.g. Keeper Unlimited). If a user's device is lost or stolen, KSI can assist in accessing encrypted backup files to restore the user's vault once the device is replaced.

Information that is stored and accessed in Keeper is only accessible by the customer because it is instantly encrypted and decrypted on-the-fly on the device that is being used - even when using the Keeper Web App. The method of encryption that Keeper uses is a well-known, trusted algorithm called AES (Advanced Encryption Standard) with a 256-bit key length. Per the Committee on National Security Systems publication CNSSP-15, AES with 256-bit key-length is sufficiently secure to encrypt classified data up to TOP SECRET classification for the U.S. Government. Keeper is FIPS 140-2 certified and validated by NIST CMVP (Certificate #3976 - **https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3976**)

The cipher keys used to encrypt and decrypt customer records are not stored or transmitted to Keeper's Cloud Security Vault. However, to provide syncing abilities between multiple devices, an encrypted version of this cipher key is stored in the Cloud Security Vault and provided to the devices on a user's account upon successful vault login and multi-factor authentication. This encrypted cipher key can only be decrypted on the device for subsequent use as a data cipher key.

Strong Master Password
It is highly recommended that customers choose a strong Master Password for their Keeper account. This Master Password should not be used anywhere outside of Keeper. Users should never share their Master Password with anyone.

Two-Factor Authentication

To protect against unauthorized access to your vault, websites, and applications, Keeper also offers Two-Factor Authentication. Two-Factor authentication is an approach to authentication requiring two or more of the three authentication factors: a knowledge factor, a possession factor, and an inherence factor.

Keeper uses something you know (your password) and something you have (the phone in your possession) to provide users extra security in the case where your master password or device is compromised. To do this, we generate TOTPs (Time-based One-Time Passwords).

Keeper generates a 10-byte secret key using a cryptographically secure random number generator. This code is valid for about a minute, and is sent to the user by SMS, Duo Security, RSA SecurID, TOTP application, Google Authenticator or Keeper DNA-compatible wearable devices like the Apple Watch or Android Wear

When using the Google Authenticator or TOTP application on your mobile device, the Keeper server internally generates a QR code containing your secret key, and it is never communicated to a third party. Each time a user deactivates, then reactivates Two-Factor Authentication, a new secret key is generated.

To activate Two-Factor Authentication, visit the Settings or Security screen of the Keeper application. Keeper Business customers can optionally enforce the use of Two-Factor Authentication to log into the vault and supported 2FA methods via the Keeper Admin Console's role enforcement functionality.

FIDO (U2F) Security Keys
Keeper supports FIDO-compatible U2F hardware-based security key devices such as YubiKey as a second factor. Security keys provide a convenient and secure way to perform two-factor authentication without requiring the user to manually enter 6-digit codes. Multiple security keys can be configured for a user's vault. For platforms that do not support security key devices, users may fall back to other configured 2FA methods. To configure a security key and other two-factor authentication methods, visit the 'Settings' screen of the Keeper application

Emergency Access (Digital Legacy)
Keeper's consumer product supports the ability to add up to 5 emergency contacts to grant vault access in the event of an emergency or death. Once a specified wait time has elapsed, the emergency contact will gain access to the user's vault. The process of sharing a vault is Zero-Knowledge, and the user's Master Password is never directly shared. RSA encryption is utilised to share a 256-bit AES key with the emergency contact, at the expiration of the wait time set by the originating user. Therefore, the emergency contact must have a Keeper account (and a public/private RSA key pair) to accept the invitation.

Account Recovery
During account signup, users may be asked to select a Security Question and Answer or another type of recovery method. Also during signup, Keeper generates a Data Key which is used to encrypt and decrypt the Record Keys stored with each of the vault records. The user's Data Key is encrypted with a key derived from the Master Password using PBKDF2 with 100,000 rounds, and each Record Key is encrypted with the Data Key. Each record in the user's vault has individual, different Record Keys.

The way account recovery works (with the Security Question method) is by storing a second copy of the user's data key that is encrypted with the selected Security Answer. To complete a vault recovery, the user is required to enter an email verification code, and also the Two-Factor Authentication code (if enabled on the account). We recommend creating a strong security question and answer, as well as turning on Keeper's Two-Factor Authentication feature from the 'Settings' screen. Different recovery methods may be available to users based on the configuration of the Keeper business account, such as a recovery key or multiple split keys. Additionally, account recovery can be disabled by the customer. Two-Factor Authentication can also be enforced for Keeper Business customers via the Keeper Admin Console.

Business and Enterprise customers are provided a zero-knowledge method of account recovery for their users using Keeper's Account Transfer policy.

Client Encryption
Data is encrypted and decrypted on the user's device, not on the Cloud Security Vault. We call this "Client Encryption" because the client (e.g. iPhone, Android Device, Desktop App, etc.) is performing local encryption and decryption of data. The Cloud Security Vault stores 256-bit encrypted ciphertext which is essentially useless to an intruder. Even if

the data is captured when it's transmitted between the client device and Cloud Security Vault, it cannot be decrypted or utilised to attack or compromise the user's private data.

Breaking or hacking a symmetric 256-bit key would require 2^{128} times the computing power of a 128-bit key. In theory, this would take a device that would require 3×1051 years to exhaust the 256-bit key space.

Sharing
Each user has a public and private 2048-bit RSA key pair that is used for sharing other keys (such as record keys, folder keys and team keys) between users. Shared information is encrypted with the recipient's public key. The recipient decrypts the shared information with their private key. This allows a user to share records only with the intended recipient, since only the recipient is able to decrypt it.

Key Generation
Keeper uses **PBKDF2** with HMAC-SHA256 to convert the user's Master Password to a 256-bit encryption key with up to 100,000 rounds. PBKDF2 iterations are based on the device platform and managed by the user in Keeper's 'Advanced Settings' screen.

Key Storage
All secret keys such as each user's RSA private key and Data Key are all encrypted prior to storage or transmission. For consumers and business users who login with a Master Password, a key is derived from the Master Password to decrypt any stored keys. For enterprise customers who login with an SSO identity provider, encrypted keys are provided to the device after successful authentication and the user's private keys are used to decrypt the Data Key and other vault keys. Since Keeper's Cloud Security Vault does not have access to the user's Master Password or encryption keys, we cannot decrypt any of your stored keys or data.

Keeper's Cloud Security Vault
The Cloud Security Vault refers to KSI's proprietary software and network architecture that is physically hosted within Amazon Web Services (AWS) infrastructure. When the user synchronizes their Keeper records with other devices on their account, the encrypted binary data is sent over an encrypted TLS tunnel and stored in Keeper's Cloud Security Vault in encrypted format.

Record Versioning
Keeper maintains full encrypted version history of every record stored in the user's vault, providing confidence that no critical data is ever lost. From the Keeper client application, users can examine the record history and perform a restore of any individual vault record. If a stored password or file in Keeper is changed or deleted, users always have the ability to perform a point-in-time restore.

Keeper Business
Customers who purchase Keeper Business are provided an extra layer of control over their users and devices. Keeper administrators are provided access to a cloud-based administrative console which allows full control over user on-boarding, off-boarding, role-based permissions, delegated administration, teams, Active Directory/LDAP integration, Two-Factor Authentication, Single Sign-On and security enforcement policies. Keeper's role-based enforcement policies are fully customizable and scalable to any sized organisation.

Record-Level Encryption
At the encryption layer, every record (e.g. password or credential) stored in the Keeper platform has a unique record identifier (Record UID). Each record is encrypted with a record key. Shared folders have a shared folder key, each team has a team key and a public/private key pair, and every user has a user data key, client key, and public/private key pair. Every role that requires the transferability of the user's account has a role enforcement key and a public/private key pair. Data at rest on the user's device is encrypted with the user's client key. The user's data key and client key are encrypted with the user's Master Password.

Records created by a user have the record key encrypted with the user's data key. Records are added to a shared folder by encrypting the record key with the shared folder key. Records are directly shared to a user by encrypting the record key with the user's public key. Users are added to a shared folder by encrypting the shared folder key with the user's public key. Teams are added to a shared folder by encrypting the shared folder key with the team's public key. Users are added to a team by encrypting the team key with the user's public key.

Roles, Teams, Shared Folders and Delegated Admin
Keeper for Business provides a secure and robust set of controls over organisational units, roles, teams and shared folders. The powerful back-end controls of Keeper provide the most robust security layers that provide least-privilege access and full delegated administration.

For Roles that enforce the transferability of a user's account:

The enforcement key is encrypted with each admins' public key that is allowed to perform the transfer. Separate enforcements applied to separate groups of users may be designated to be transferred by separate groups of admins.

The user's data key (for users in a role to which the enforcement is applied) is encrypted with the role enforcement's public key (Referenced below as the user's shared data key).

An account to be transferred is performed by locking then transferring and deleting a user's account. This ensures the operation is not performed secretly. The user's shared data key is retrieved by the admin and decrypted. This is used to decrypt all the record keys, team keys, and folder keys the transferred user had access to and those keys are shared with the public key of the user being transferred to. The admin does not receive the record and folder data, but instead simply transferred the keys. Only the recipient gets access to the record and folder data.

All encryption is performed client side, and at no time does Keeper have the ability to decrypt the information being shared or transferred. Additionally, at no time is a user's client key shared. Therefore, the data cached on a user's device cannot be decrypted without the user's master password. A user who is removed from a team, shared folder, or direct share will not receive new data from the team, shared folder, or record. Although the record, folder and team keys are compromised to the admin, the keys are not usable for gaining access to the underlying record or folder data.

Several different administrative privileges may be assigned to portions of a hierarchical tree that allows the members of the privileged role to perform operations in our Keeper Admin Console.

Server-side and client-side enforcement policies may also be applied to roles to dictate the behavior of the client for groups of individuals.

Teams enables easy distribution of shared folders to groups of users.

Permission protection and encryption protection are two very different models of our security. Because permission protection does not require the exchange of keys, permissions could be changed by Keeper personnel with sufficient authority such that a user who cannot edit a record he/she has access to could be given the ability to edit the record. Once a key is compromised with a user it becomes a matter of permission for the underlying data, not encryption.

Keeper Active Directory / LDAP Bridge
The Keeper Bridge integrates with Active Directory and LDAP servers for provisioning and onboarding of users. Keeper Bridge communication is first authorised by an admin with the privilege to manage the bridge. A transmission key is generated and shared with Keeper for all subsequent communication. The use of the transmission key is the authorization for all operations performed by the bridge except for the initialization of the Bridge. The transmission key may be regenerated at any time, and it will automatically rotate every 30 days.

The transmission key is only for transmission which means a compromised key may be reinitialised or revoked without any loss of data or permission.

Keeper Bridge may not give privileges to a role or user. It may add a user to a privileged role, as long as no enforcement keys are needed. Keeper Bridge may not elevate itself or a user above the portion of the tree it is managing. Not all operations are available to the Bridge, i.e. the Bridge can disable an active user, but may not delete the user. The admin will have to choose if the user is to be deleted or transferred.

Single Sign-On (SAML 2.0) authentication
Keeper can be configured by Keeper Business customers to authenticate a user into their Keeper vault using standard SAML 2.0 identity products. Keeper is a pre-configured service provider in every major SSO Identity Provider such as Google Apps, Microsoft Azure, Okta, Ping Identity and others. The mechanism that Keeper utilises to authenticate users

into their vault in a Zero-knowledge environment is the patent-pending implementation called Keeper SSO Connect®. Keeper SSO Connect® is a software application that Keeper Business administrators install on their own infrastructure (either on-premise or cloud), which serves as a SAML 2.0 service provider endpoint. When activated on a particular organisational unit, Keeper SSO Connect® manages all of the encryption keys for Keeper Business end-users. Upon successful authentication in to the business Single Sign-On Identity Provider, the user is logged into Keeper with the necessary encryption keys to decrypt their vault. Keeper SSO Connect® software operates on Windows, Mac and Linux environments.

SSO Connect® Cloud
Keeper SSO Connect® Cloud provides Keeper Enterprise customers with a method of authenticating a user and decrypting stored data in a zero-knowledge encrypted vault, with authentication provided through a 3rd party identity provider (IdP) utilising standard SAML 2.0 protocols in a fully cloud environment.

In this implementation, a user can authenticate through their SSO identity provider and then decrypt the ciphertext of their vault locally on their device. Each device has its own EC (Elliptic Curve) public/private key pair and encrypted data key. Each user has their own Data Key. To sign into a new device, the user must utilise existing devices to perform an approval or an administrator with the privilege can approve a new device.

The importance of this capability is that the user can decrypt their vault using an encrypted key stored in the Keeper cloud. Zero knowledge is preserved because the Keeper cloud is unable to decrypt the user's Data Key on their device. The Data Key ("DK") of the user is decrypted with the device private key ("DPRIV"), and the Encrypted Data Key ("EDK") is only provided to the user upon successful authentication from their designated identity provider (e.g. Okta, Azure, AD FS).

For SSO Connect® Cloud users, an Elliptic Curve private key is generated and stored locally on each device. For Chromium-based web browsers, the Keeper Vault stores the local device EC private key ("DPRIV") as a non-exportable CryptoKey. On iOS and Mac devices, the key is stored in the device KeyChain. Where available, Keeper utilises secure storage mechanisms.

The Device Private Key is not directly utilised to encrypt or decrypt vault data. Upon successful authentication from the Identity Provider, a separate key (that is not stored) is utilised for decryption of the vault data. Offline extraction of the local Device Private Key cannot decrypt a user's vault.

Different devices/platforms have varying levels of security, and so in order to provide optimal security we recommend using an up-to-date Chromium-based web browser.

As general protection against compromised device attacks, we also recommend that all devices (such as desktop computers) are protected with disk-level encryption and up-to-date anti-malware software.

SSO Device Approvals
To sign into a new device, the user must utilise existing devices to perform an approval or an administrator with the privilege can approve a new device. New devices generate a new set of public/private keys, and the approving device encrypts the user's data key with the public key of the new device. The new device's encrypted data key (EDK) is provided to the requesting user/device and then the user is able to decrypt their data key, which then decrypts the user's vault data. Within the decrypted vault data the user can decrypt their other private encryption keys such as record keys, folder keys, team keys, etc.

The importance of this capability is that the user can decrypt their vault using an encrypted key stored by the Keeper cloud, and does not require any on-prem or user-hosted application services to manage the encryption keys. Zero knowledge is preserved because the Keeper cloud is unable to decrypt the user's Data Key on their device. The Data Key of the user is decrypted with the device private key (DPRIV), and the EDK is only provided to the user upon successful authentication from their designated identity provider (e.g. Okta, Azure, AD FS).

From an administrator's perspective, the benefits are: easy setup and no required hosted software to manage encryption keys as described in Keeper's current SSO Connect® encryption model. The only workflow change in this model (compared to on-prem implementation of Keeper SSO Connect®) is that the user must perform new device approval on an active device, or delegate the responsibility to a Keeper Administrator to perform device approval.

Keeper SSO Connect® On-Prem
SSO Connect® On-Prem is a self-hosted integration that requires either a Windows or Linux hosted application server. In order to maintain Zero Knowledge security and ensure a seamless SSO experience for users, Keeper SSO Connect® must be installed on the customer's server. Windows, Mac and Linux environments are fully supported with High Availability (HA) load balancing operational modes.

Keeper SSO Connect® automatically generates and maintains the Master Password for each provisioned user, which is a randomly generated 256-bit key. This Master Password is encrypted with the SSO Key. The SSO Key is encrypted with the Tree Key. The SSO Key is retrieved from the server upon Keeper SSO Connect® service startup, and then decrypted using the Tree Key, which is stored locally on the server to support automatic service startup. Communication between SSO Connect® and Keeper's Cloud Security Vault is protected with a Transmission Key. SAML communications are cryptographically signed and are protected by the RSA-SHA256 or ECDSA-SHA256 signature algorithm depending on the type of encryption key (RSA or EC) provided by the customer.

BreachWatch
BreachWatch constantly scans Keeper records against public data breaches and alerts the user within the vault. BreachWatch is a Zero Knowledge architecture that uses a number of layered techniques to protect our customer's information. In summary:

1. A secure, keyed, cryptographic hash function and anonymisation are used to perform a comparison of passwords against a database of breached account information.

2. Customer passwords are processed with a hardware security module (HSM) and a non-exportable secret key before being checked against breached passwords or stored on BreachWatch servers.

3. Keeper customers interact with BreachWatch using anonymised BreachWatch IDs that are unlinked from other Keeper customer identifiers.

4. BreachWatch separates usernames and passwords into separate services with distinct, anonymised IDs to unlink usernames and domains from passwords.

5. BreachWatch customers never upload domain information; only downloading domains.

The path of a customer's hashed password data through BreachWatch. Only passwords hardened with an HSM and a non-exportable key are stored on BreachWatch servers. BreachWatch customers use anonymised IDs when interacting with BreachWatch servers.

To build a secure service, Keeper split BreachWatch into three services; one each for checking domains, usernames, passwords and username+password pairs. Keeper client applications contact each of these backend services using an encrypted REST API.

Domain Scanning
BreachWatch customers download a list of domains that have been breached and perform the checking locally.

Username and Password Scanning
Client devices connect to BreachWatch and upload a list of hashed usernames (or passwords) along with a client-selected, random identifier (separate identifiers for the username- and password-checking services). These password hashes are processed on upload with HMAC using a hardware security module (HSM) and a secret key stored in the HSM marked as non-exportable (meaning the HSM will only process the HMAC locally and the key cannot be extracted). These HMAC'd inputs (usernames or passwords) are compared against the breach datasets which have been processed with the same HMAC and key. Any matches are reported to the client device. Any values that don't match are stored alongside the client's anonymised ID.

As new breached usernames and passwords are added to the system, they are processed with HMAC on the HSM, added to the BreachWatch dataset, and compared against the stored client values. Any matches queue an alert for that client ID.

Clients check-in periodically to BreachWatch and present their BreachWatch IDs. Any queued messages are downloaded and clients upload any new or changed usernames and passwords which are processed the same way.

Security of the BreachWatch services is trust-on-first-use (TOFU). That is, clients must assume that the BreachWatch server is not malicious (that is, not actively compromised by an attacker) when the client uploads their hashed values. Once these values are processed with an HSM they are secured against offline cracking attempts. In other words, if an attacker steals the dataset of stored client values, they cannot crack those values offline without the HMAC key stored in the HSM.

If a breach of a password is detected, the client device sends a username+password combination hash to the BreachWatch servers which then performs the same HMAC hash comparison to determine if a combination of username+password was breached, and if so, the domains related to those breaches are returned so the client device can determine if username+password+domain is matched. If all three parameters match on the client device, the user is alerted as to the severity of the breach.

BreachWatch Business
When BreachWatch is activated for business and enterprise customers, the end-user vaults are scanned automatically, every time a users logs in with Keeper. The BreachWatch summary data scanned on the user's device is encrypted with the Enterprise public key and decrypted by the enterprise administrator when logging into the Keeper Admin Console. This encrypted information includes the email address, number of high-risk records, number of resolved records and number of ignored records. The Keeper administrator is able to view user-level summary statistics within the Admin Console user interface.

Event Logging and Reporting
When integrated with the Advanced Reporting & Alerts module, Keeper end-user devices may also be optionally configured to transmit detailed real-time events into 3rd party SIEM solutions and the Keeper Admin Console reporting interface. The event data contains email address, record UID, IP address and device information (events do not include any decrypted record data, since Keeper is a Zero-Knowledge platform and cannot decrypt user data).

By default, detailed BreachWatch event data is not sent to the Advanced Reporting & Alerts Module or any connected external logging systems. To activate event-level reporting of BreachWatch data to the Advanced Reporting & Alerts Module you must enable the event role enforcement policy under the specific role > Enforcement Policies > Vault Features screen. Once activated, the end-user client devices will begin sending this event data. Since integration with 3rd party SIEM solutions is transmitted from the Keeper backend to the target SIEM, this event information is therefore readable by the target SIEM and could be used to identify which records and which users within the organisation have high-risk passwords. If the Keeper Administrator does not wish to transmit record-level event data to the Keeper Advanced Reporting & Alerts Module, this setting can be left disabled.

Offline Mode
Offline Mode allows users to have access to their vault when they are not able to connect online to Keeper or to their SSO Identity Provider. This capability is available on Keeper's mobile app, desktop application and extended to Business users on popular web browsers.

The capability works by making a copy of the vault to the user's local device. The vault data stored offline is AES-GCM encrypted with a 256-bit “Client Key” that is generated randomly and protected by PBKDF2-HMAC-SHA512 with up to 100,000 iterations and a random salt. The salt and iterations are stored locally. When the user enters their Master Password, a key is derived using the salt and iterations and an attempt is made to decrypt the Client Key. The Client Key is then used to decrypt the stored record cache. If Self-Destruct protection is enabled on the user's vault, 5 failed attempts to login will automatically wipe all locally stored vault data.

Network Architecture
KSI utilises Amazon AWS in North America, Europe and Australia, for localised data privacy and geographic segregation to host and operate the Keeper solution and architecture. Utilizing Amazon AWS allows Keeper to seamlessly scale resources on-demand and provide customers with the fastest and safest cloud storage environment.

KSI operates both multi-zone and multi-region environments to maximize uptime and provide the fastest response time to customers.

Server Authentication
The Keeper Cloud Security Vault is protected by an API which authenticates each request from the client device. On the client device, a 256-bit "Authentication Key" is derived from the Master Password using PBKDF2-HMAC-SHA256 and a random salt. An "Authentication Hash" is generated by hashing the "Authentication Key" using SHA-256. To login, the Authentication Hash is compared against a stored Authentication Hash on the Cloud Security Vault. After login, a session token is generated and used by the client device for subsequent requests. This authentication token must be renewed every 30 minutes, or upon the request of the server.

Transport Layer Encryption
KSI supports 256-bit and 128-bit TLS to encrypt all data transport between the client application and KSI's cloud-based storage. This is the same level of encryption trusted by millions of individuals and businesses everyday for web transactions requiring security, such as online banking, online shopping, trading stocks, accessing medical information and filing tax returns.

KSI deploys TLS certificates signed by Digicert using the SHA2 algorithm, the most secure signature algorithm currently offered by commercial certificate authorities. SHA2 is significantly more secure than the more widely used SHA1, which could be exploited due to mathematical weakness identified in the algorithm. SHA2 helps protect against the issuance of counterfeit certificates that could be used by an attacker to impersonate a website.

KSI also supports Certificate Transparency (CT), a new initiative by Google to create a publicly auditable record of certificates signed by certificate authorities. CT helps guard against issuance of certificates by unauthorised entities. CT is currently supported in the latest versions of the Chrome web browser. More information about Certificate Transparency can be found at: **https://www.certificate-transparency.org**. Keeper supports the following TLS cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Key Pinning
Keeper's native clients implement clients implement Key Pinning, a security mechanism which prevents impersonation by attackers using fraudulent digital certificates.

Cross-Site Scripting (XSS) Attack Protection
The Keeper Web Vault implements a strict Content Security Policy that restricts the origin of outbound requests and prevents all scripts from being executed, except those explicitly sourced from Keeper, including inline scripts and event-handling HTML attributes, reducing or eliminating most vectors for cross-site scripting attacks.

Access to the KeeperSecurity.com and KeeperSecurity.eu domain names is restricted to HTTPS with TLS v1.2 and is enforced by HTTP Strict Transport Security. This prevents a wide array of packet sniffing, data modification, and man-in-the-middle attacks.

Within the Keeper Browser Extension, Keeper will not prompt users to login to their vault from within the page frame area. Login to the extension occurs within the Browser Extension toolbar area of the browser. Login to the vault on the web browser will always occur either on the KeeperSecurity.com domain, KeeperSecurity.eu domain or from the Keeper browser extension toolbar which exists outside of the content page.

The Keeper Browser extension on Chrome, Firefox, Edge and Opera utilise iFrames for injection of record data on the login screens of websites to ensure that no malicious website has access to injected content. Record content injected into iFrames is also limited to the vault records stored in the user's vault which match the domain of the target website. Keeper will not offer Autofill of login or password data unless the website domain matches the website domain field of the Keeper vault record.

The Internet Explorer Extension uses a separate native application window for logging in and accessing records. These separate windows are not subject to XSS attacks because they are not accessible from the browser. This allows the Extension in Internet Explorer to provide a login window from inside the page. The extension will not show records unless the records match the website address root domain.

3rd party browser extensions may have elevated permissions in web browsers and can access information within the page. Therefore, it is recommended that Keeper administrators prevent users from installing unapproved 3rd party browser extensions from the browser's respective app store.

iOS Keychain, Touch ID® and Face ID®
Touch ID and Face ID on iOS devices allows you to access your Keeper vault using your biometrics. To provide this convenient feature, a randomly generated 256-bit "biometric key" is stored in the iOS Keychain. The iOS Keychain item created for this functionality is not designated to synchronize to the iCloud Keychain and thus will not leave your iOS mobile device.

It is highly recommended that you use a complex Master Password and enable Multi-factor authentication in order to provide maximum security for your encrypted Keeper Vault. Using Touch ID and Face ID makes it more convenient to use a complex Master Password on your iOS mobile device. It is also recommended that you set a passcode longer than the minimum 4-digits to secure the iOS Keychain.

The iOS Keychain is used by iOS and apps to securely store credentials. iOS apps use the iOS Keychain to store a variety of sensitive information, including website passwords, keys, credit card numbers and Apple Pay™ information. Keeper does not use the iOS Keychain to store your Keeper records - all Keeper records are protected with 256-bit AES encryption and are securely stored in the Keeper Vault. The iOS Keychain is also encrypted with 256-bit AES encryption using the device's passcode. Even if the device is lost or stolen or an attacker obtains physical access to the mobile device, they will be unable to access any stored Keeper information. The iOS Keychain cannot be decrypted without the passcode and the Keeper Vault cannot be decrypted without the user's Keeper Master Password.

Biometrics
Keeper natively supports Windows Hello, Touch ID, Face ID and Android biometrics. Customers who normally login to their Keeper Vault using a Master Password or Enterprise SSO Login (SAML 2.0) can also login to their devices using a biometric. Biometrics must be enabled by the Keeper Administrator in the role policy. Offline access can also be achieved with a biometric for both Master Password and SSO-enabled users when this feature is activated.

When biometric login is enabled on a device, a key is randomly generated locally and stored in the secure enclave (e.g. Keychain) of the device. The user's Data Key is encrypted with the biometric key. Upon successful biometric authentication, the key is retrieved and the user is able to decrypt their vault.

Apple Watch®
The Apple Watch Favourite feature allows the viewing of selected records on a paired Apple Watch. Keeper records must be explicitly enabled to allow viewing on the Apple Watch. A paired Apple Watch communicates with the Keeper Watch Extension that transparently runs in a sandboxed space separate from the iOS Keeper App. The Keeper Watch Extension also uses iOS Keychain to securely store and access keys to enable it to seamlessly and securely communicate with the iOS Keeper app.

Keeper DNA®
Keeper DNA is a new and innovative addition to multi-factor authentication. When used with a paired Apple Watch, Keeper DNA provides a multi-factor authentication method that is unparalleled in convenience and security. Keeper DNA uses secure tokens stored in the Keeper Vault to generate time-based codes for multi-factor authentication. These time-based authentication requests can be approved and sent automatically from the Apple Watch (or Android Wear device) with a tap on the screen of the watch or entered manually by the user. Multiple layers of encryption, Touch ID and multi-factor authentication help make Keeper DNA the most elegant, secure and advanced authentication method available.

Compliance & Audits

Certified SOC 2 Compliant

Customer data is protected using stringent and tightly monitored internal control practices. Keeper is certified as SOC 2 Type 2 compliant in accordance with the AICPA Service Organization Control framework. SOC 2 certification helps ensure that your data is kept secure through the implementation of standardised controls as defined in the AICPA Trust Service Principles framework.

ISO 27001 Certified (Information Security Management System)
Keeper is ISO 27001 certified, covering the Keeper Security Information Management System which supports the Keeper Enterprise Platform. Keeper's ISO 27001 certification is scoped to include the management and operation of the digital vault and cloud services, software and application development, and protection of digital assets for the digital vault and cloud services.

GDPR Compliance
Keeper is GDPR compliant and we are committed to ensuring our business processes and products continue to maintain compliance for our customers in the European Union.

Protection of Patient Medical Data
Keeper software is compliant with global, medical data protection standards covering, without limitation, HIPAA (Health Insurance Portability and Accountability Act) and DPA (Data Protection Act).

HIPAA Compliance and Business Associate Agreements
Keeper is a SOC2-certified and ISO 27001-certified zero-knowledge security platform that is HIPAA compliant. Strict adherence and controls covering privacy, confidentiality, integrity and availability are maintained. With this security architecture, Keeper cannot decrypt, view or access any information, including ePHI, stored in a user's Keeper Vault. For the foregoing reasons, Keeper is not a Business Associate as defined in the Health Insurance Portability and Accountability Act (HIPAA), and therefore, is not subject to a Business Associate Agreement.

To learn more about the additional benefits for healthcare providers and health insurance companies, please read this entire Security Disclosure and visit our **Enterprise Guide**.

Penetration Testing
Keeper performs periodic pen testing with 3rd party experts including **NCC Group**, **Secarma**, **Rhino Security**, **Cybertest** and independent security researchers against all of our products and systems. Keeper has also partnered with Bugcrowd to manage its vulnerability disclosure program (VDP).

Third-Party Security Scanning & Penetration Tests
KSI is tested daily by McAfee Secure to ensure that the Keeper web application and KSI's Cloud Security Vault are secure from known remote exploits, vulnerabilities and denial-of-service attacks. McAfee Secure badges may be found on the Keeper website to verify daily testing of the Keeper website, Web application, and Cloud Security Vault.

A comprehensive external security scan is conducted monthly on the Keeper website, Keeper web application, and Keeper Cloud Security Vault by McAfee Secure. Keeper staff periodically initiate on-demand external scans through McAfee Secure.

Payment Processing and PCI Compliance
KSI uses PayPal and Stripe for securely processing credit and debit card payments through the KSI payment website. PayPal and Stripe are PCI-DSS compliant transaction processing solutions.

KSI is certified PCI-DSS compliant by McAfee Secure.

EU-US Privacy Shield
The Keeper web client, Android App, Windows Phone App, iPhone/iPad App and browser extensions have been certified EU Privacy Shield compliant with the U.S. Department of Commerce's EU-U.S. Privacy Shield program, meeting the European Commission's Directive on Data Protection.
For more information about the U.S. Department of Commerce U.S.-EU Privacy Shield program, see **https://www.privacyshield.gov**

FIPS 140-2 Validated

Keeper utilises FIPS 140-2 validated encryption modules to address rigorous government and public sector security requirements. Keeper's encryption has been certified by the NIST CMVP and validated to the FIPS 140 standard by accredited third party laboratories. Keeper has been issued **certificate #3967** under the NIST CMVP

U.S. Department of Commerce Export Licensed Under EAR
Keeper is certified by the U.S. Department of Commerce Bureau of Industry and Security under Export Commodity Classification Control Number 5D992, in compliance with Export Administration Regulations (EAR). For more information about EAR: **https://www.bis.doc.gov**

24x7 Remote Monitoring
Keeper is monitored 24x7x365 by a global third-party monitoring network to ensure that our website and Cloud Security Vault are available worldwide.

If you have any questions regarding this security disclosure, please **contact us**.

Phishing or Spoofed Emails
If you receive an email purporting to be sent from KSI and you are unsure if it is legitimate, it may be a "phishing email" where the sender's email address is forged or "spoofed". In that case, an email may contain links to a website that looks like KeeperSecurity.com but is not our site. The website may ask you for your Keeper Security master password or try to install unwanted software on your computer in an attempt to steal your personal information or access your computer. Other emails contain links that may redirect you to other potentially dangerous web sites. The message may also include attachments, which typically contain unwanted software called "malware." If you are unsure about an email received in your inbox, you should delete it without clicking any links or opening any attachments.

If you wish to report an email purporting to be from KSI that you believe is a forgery or you have other security concerns involving other matters with KSI, please **contact us**.

Hosting Infrastructure Certified to the Strictest Industry Standards
The Keeper website and cloud storage runs on secure Amazon Web Services (AWS) cloud computing infrastructure. The AWS cloud infrastructure which hosts Keeper's system architecture has been certified to meet the following third-party attestations, reports and certifications:

- SOC 1/ SSAE 26/ISAE 3402 (SAS70)
- SOC 3
- SOC 3
- PCI DSS Level 1
- ISO 27001
- FedRamp
- DIACAP
- FISMA
- ITAC
- FIPS 140-2
- CSA
- MPAA

Vulnerability Reporting and Bug Bounty Program

Keeper Security is committed to the industry best practice of responsible disclosure of potential security issues. We take We take your security and privacy seriously are committed to protecting our customers' privacy and personal data. KSI's mission is to build world's most secure and innovative security apps, and we believe that bug reports from the worldwide community of security researchers is a valuable component to ensuring the security of KSI's products and services.

Keeping our users secure is core to our values as an organisation. We value the input of good-faith researchers and believe that an ongoing relationship with the cybersecurity community helps us ensure their security and privacy, and makes the Internet a more secure place. This includes encouraging responsible security testing and disclosure of security vulnerabilities.

Guidelines
Keeper's Vulnerability Disclosure Policy sets out expectations when working with good-faith researchers, as well as what you can expect from us.
If security testing and reporting is done within the guidelines of this policy, we:

- Consider it to be authorised in accordance with Computer Fraud and Abuse Act,
- Consider it exempt from DMCA, and will not bring a claim against you for bypassing any security or technology controls,
- Consider it legal, and will not pursue or support any legal action related to this program against you,
- Will work with you to understand and resolve the issue quickly, and
- Will recognise your contributions publicly if you are the first to report the issue and we make a code or configuration change based on the issue.

If at any time you are concerned or uncertain about testing in a way that is consistent with the Guidelines and Scope of this policy, please contact us at **security@keepersecurity.com** before proceeding.
To encourage good-faith security testing and disclosure of discovered vulnerabilities, we ask that you:

- Avoid violating privacy, harming user experience, disrupting production or corporate systems, and/or destroying data,
- Perform research only within the scope set out by the Bugcrowd vulnerability disclosure program linked below, and respect systems and activities which are out-of-scope,
- Contact us immediately at security@keepersecurity.com if you encounter any user data during testing, and
- You give us reasonable time to analyse, confirm and resolve the reported issue before publicly disclosing any vulnerability finding.

Submitting a Report
Keeper has partnered with Bugcrowd to manage our vulnerability disclosure program.

Please submit reports through **[https://bugcrowd.com/keepersecurity]**.

Additional Information

Product Documentation
Keeper's documentation portal containing product manuals, technical information, release notes and end-user guides is available at: **https://docs.keeper.io**

System Status
Realtime system status can be found at: **https://statuspage.keeper.io**