

DATA PROCESSING ADDENDUM

This Data Processing Addendum is agreed to and incorporated into, and is subject to the contractual language in the Agreement between Kandji, Inc. (“Kandji”, “the data importer”) and the Corporate Customer (“the data exporter”) that is a party to the Agreement. All references to the “Agreement” in this document shall include the Data Processing Addendum as detailed herein.

1. Definitions

“**Agreement**” means all legal documents collectively signed by the parties governing the legal relationship between the parties.

“**Corporate Customer**” means the data exporter and data controller using the Service provided by Kandji and named in the Agreement.

“**Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

“**Data Controller**” means the Corporate Customer, which shall determine the purpose and means of the processing of Personal Data.

“**Data Subjects**” means individuals located in the EEA for whom Kandji is processing personal information on behalf of the Corporate Customer.

“**Data Processor**” means Kandji, Inc.

“**EEA**” means the European Economic Area.

“**GDPR**” means the General Data Protection Regulation.

“**Personal Data**” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

“**Sensitive Data**” means the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

“**Service**” means the mobile device management service offered by Kandji to Corporate Customer.

“**Standard Contract Clauses**” mean standard contract clauses applicable to the transfer of data to processors not located in the EEA and Switzerland as established and approved by the European Commission or Switzerland Data Protection Authority.

“**Sub-Processor**” means any processor engaged by Kandji to assist in providing this Service to the Corporate Customer.

“**Supervisory Authority**” means a public agency or authority established by a Member State of the European Union to enforce the GDPR.

2. EEA Applicability

This Data Processing Addendum shall apply only to the extent Corporate Customer or Data Subjects accessing the Service through its account are located within the EEA and the Data Processor processes Personal Data of the Corporate Customer or Data Subjects.

3. Data Processing Specifications

(a) **Subject Matter.** The subject matter of data processed under this Data Processing Agreement is Personal Data of the representatives of Corporate Customers and Data Subjects using authorized devices in the account of the Corporate Customer with Kandji.

(b) **Purpose of Processing.** Kandji shall only process Personal Data to provide the Service to Corporate Customer and users of authorized devices in the account of Corporate Customer; to respond to inquiries from Corporate Customer or Data Subjects using authorized devices in the account of Corporate Customer; and to comply with any additional instructions provided by Corporate Customer from time-to-time.

(c) **Duration of Processing.** Kandji shall process Personal Data so long as Corporate Customer remains a client. Upon termination of the Service by either party, Kandji shall cease processing Personal Data upon completion of the termination provisions described herein.

(d) **Nature of Processing.** Kandji provides a mobile device management service wherein Corporate Customer can administer authorized mobile devices in its account. Kandji will process the Personal Data of Data Subjects to associate such individuals with specifically authorized devices and apply the Service.

(e) **Categories of Data Subjects:** The categories of data subjects include 1) representatives of Corporate Customer interacting with Kandji, and 2) users of authorized devices in the account of Corporate Customer.

(f) **Customer Data.** Representative of Corporate Customer may provide Kandji with contact information, payment information, and identifying information such as name and location. Users of authorized devices may provide their identity, proof of authorization, mobile device identification information, and be identified by their authorized device.

(g) **Sensitive Data.** Kandji does not process sensitive data as defined in Article 9 of the GDPR and Corporate Customer agrees not to instruct Kandji to do so.

(h) **Processing Operations.** Personal Data will be processed by Kandji pursuant to this Data Protection Agreement and supporting documentation in that it will be stored, organized, and made available to Corporate Customer as the Data Controller.

4. Corporate Customer Instructions – Data Processing

(a) Instructions. Corporate Customer appoints Kandji to process the Personal Data of Data Subjects on the Data Controller's behalf in conjunction with the Service provided herein only as is necessary to provide such Service. Corporate Customer shall designate Data Subjects authorized to use devices in Corporate Customer's account with Kandji and instruct Kandji on mobile device management of said devices and Personal Data as detailed in the original Agreement between the party, this Data Processing Addendum, Standard Contract Clauses annexed hereto, and subsequent instructions provided by Corporate Customer.

(b) Lawful Basis. The Corporate Customer warrants and guarantees it has established a lawful basis pursuant to the GDPR for the processing of the Personal Data of Data Subjects using authorized devices in the account of Corporate Customer.

(c) Limited Kandji Processing. Kandji will only process the Personal Data of Data Subjects using authorized devices in the account of Corporate Customer pursuant to the scope detailed in the Agreement between the parties and any additional instructions specifically provided by Corporate Customer.

(d) Data Security. Kandji maintains appropriate data security measures as detailed in the Annex of Standard Contract Clauses of this Data Processing Addendum. Kandji will ensure only employees, personnel, and sub-processors who work with such Personal Data will be bound by appropriate obligations of confidentiality. Corporate Customer is solely responsible for making an independent determination as to whether the Services meet Corporate Customer's requirements and legal obligations under relevant laws including, but not limited to, data privacy laws in the EEA and Switzerland. Corporate Customer further agrees to be solely responsible for the secure use of the Services by itself and any individual it provides with an authorized device, including securing account authentication information and ensuring no authorized user seeks to misuse Personal Data or create a Data Breach.

(e) Kandji Cooperation. Kandji will reasonably cooperate with Corporate Customer and provide assistance as called for in Articles 32 through 36 of the GDPR. Kandji will provide Corporate Customer with prompt notice of any complaint or request received from a Supervisory Authority or Data Subject in relation to data privacy issues no less than two business days after receiving the communication based on Pacific Standard Time Zone in San Diego, California, United States.

(f) Data Policy Upon Termination. Should Corporate Customer terminate its relationship with Kandji or Kandji terminate the account of Corporate Customer, Personal Data processed through the account of Corporate Customer shall be handled in the following manner as chosen by Corporate Customer:

- i. Returned to the Corporate Customer,
- ii. Deleted and destroyed by Kandji, or
- iii. Rendered anonymously such that it no longer is considered Personal Data under the GDPR.

(g) Sensitive Data. Corporate Customer agrees it will not transfer or make available for transfer any Sensitive Data. The parties agree that Kandji will have no liability for events, including data breaches, involving Sensitive Data pursuant to this Data Protection Addendum.

(h) Additional Allowed Uses. Kandji shall have the right to collect and use Personal Data for administrative purposes such as accounting and compliance; to investigate a use of the Service that is

unlawful or violates the Agreement entered into by the parties; to provide and develop the Service, and to respond to legal actions.

5. Cross-Border Data Transfers

Pursuant to the requirements of Article 46(1) and (2)(c) of the GDPR, the parties agree that Standard Contract Clauses found in Annex A, which are incorporated by reference into this Data Processing Addendum, shall govern the transfer of Personal Data out of the EEA and Switzerland for processing by Kandji and, where it occurs, the Corporate Customer.

6. Data Breach

Pursuant to Article 33(2) of the GDPR, Kandji will notify Corporate Customer of any data breach impacting Personal Data processed through the account of Corporate Customer without undue delay after becoming aware of the data breach.

7. Kandji Sub-Processors

Corporate Customer provides Kandji with general written authorization to engage a sub-processor pursuant to Article 28(2) of the GDPR. Kandji shall inform Corporate Customer of any intended changes concerning additional or replacement processors, and give Corporate Customer the right to object to such changes within five (5) business days of such notice.

8. Demonstrable Compliance

Kandji will make available to the Corporate Customer all information necessary to demonstrate compliance with the obligations in this Data Processing Agreement and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. Corporate Customer agrees it will provide no fewer than thirty (30) days written notice of its intent to exercise these demonstrable compliance rights; agrees to conduct such audit during Kandji's normal business hours at Kandji's headquarters in a manner that does not reasonably interfere with Kandji's normal business operations; and the audit shall last no more than sixteen (16) consecutive business hours from nine (9) in the morning through five (5) in the evening Pacific Standard Time. The parties further agree that Corporate Customer shall have no right to the proprietary or confidential information or company property of Kandji other than to the extent to show demonstrable compliance as detailed in this section. Should the parties disagree on the disclosure of particular material or information, they shall submit the dispute to the San Diego Superior Court through an agreed upon legal notice or, if not agreed up, a Declaratory Relief Action which shall stay the audit at the time of the filing of the Action. Corporate Customer further agrees to reimburse Kandji for its reasonable costs associated with cooperating with the audit, inspection or other action taken by Corporate Customer to determine demonstrable compliance.

9. Conflicting Documentation

Corporate Customer and Kandji have entered into an Agreement consisting of multiple legal documents. To the extent these documents or the language within them conflict, the following documents shall govern in descending order:

- Standard Contract Clauses

- Data Processing Addendum
- CCPA Addendum
- Terms of Use
- General Privacy Policy

10. Subpoenas and Court Orders

Kandji shall make a reasonable attempt to redirect any subpoenas or other legal notices to Corporate Customer. Kandji will give Corporate Customer reasonable notice if legal authorities seek to compel Kandji to produce information or Personal Data unless Kandji is prevented from doing so as a matter of law or in its sole determination that it is prevented from doing so under law.

The parties authorized signators duly execute this Agreement as follows:

Corporate Customer

Signed: _____

Name: _____

Title: _____

Date: _____

Kandji, Inc.

Signed:  _____

Name: Mark Daughters

Title: Head of Operations

Date: 03/11/2020

Annex A - Standard Contract Clauses

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

Data Exporting Organization:

[The Corporate Customer as defined in the Agreement between the parties or identified as the following]

[CUSTOMER FILL OUT]

Name: _____

Address: _____

Fax, if any: _____

Phone Number: _____

E-mail: _____

(the data exporter)

Data Importing Organization:

Kandji, Inc.

101 W. Broadway, Suite 1130

San Diego, California 92101

No Fax

Phone Number: (855) 877-1866

legal@kandji.com

(the data importer)

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 Appendix A.

1. Definitions

For the purposes of the Clauses:

a) personal data, special categories of data, process/processing, controller, processor, data subject and supervisory authority shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

b) **the data exporter** means the controller who transfers the personal data – the Corporate Customer;

c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Data Processing Addendum and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix A which forms an integral part of the Data Processing Addendum.

3. Third-party beneficiary clause

The data subject can enforce against the data exporter this clause 3, clause 4.1(b) to clause 4.1(i), clause 5.1(a) to clause 5.1(e) and clause 5.1(g) to clause 5.1(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

The data subject can enforce against the data importer this clause, clause 5.1(a) to clause 5.1(e) and clause 5.1(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.1 The data subject can enforce against the sub-processor this clause 3.1, clause 5.1(a) to clause 5.1(e) and clause 5.1(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

- a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix B to this contract;
- d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e) that it will ensure compliance with the security measures;
- f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5.1(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix B and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and
- j) that it will ensure compliance with clause 4.1(a) to clause 4.1(i).

5. Obligations of the data importer

The data importer agrees and warrants:

- a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c) that it has implemented the technical and organisational security measures specified in Appendix B before processing the personal data transferred;
- d) that it will promptly notify the data exporter about:
- i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - ii. any accidental or unauthorised access; and
 - iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and
- j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5.1(b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

The parties authorized signators duly execute this Agreement as follows:

Corporate Customer

Signed: _____

Name: _____

Title: _____

Date: _____

Kandji, Inc.

Signed:  _____

Name: Mark Daughters

Title: Head of Operations

Date: 03/11/2020

APPENDIX A – DATA INFORMATION

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix A.

Data exporter

The data exporter is the party listed as the “Corporate Customer” in the Agreement between the parties.

Data importer

The data importer is Kandji, Inc., a technology company providing mobile device management services to companies.

Data subjects

The personal data transferred concern the employees and individuals the Corporate Customer allows to use authorized devices in its account with Kandji, Inc.

Categories of data

The personal data transferred concern the following categories of data:

- Name,
- Photograph for some, not all, individuals,
- Unique identifier for authorized device being used,
- Filtering of programs which configuration may indirectly be used to identify a person, and
- Communications from the individual in question.

Special categories of data

Special categories of data are not transferred between the data exporter and data importer.

Processing operations

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

- Identifying users of authorized devices in Corporate Customer accounts.
- Processing legal requests under privacy laws such as the California Consumer Protection Act.
- Facilitating the organization of program designations by Corporate Customers to its users.
- Responding to communications from Corporate Customer representatives and users of Authorized Devices.

Categories of Data Subjects

- The users of authorized devices in the account of the Corporate Customer.

- The data exporter representatives.

Duration

Processing will continue for the duration of the Agreement between Corporate Customer and Kandji.

APPENDIX B – TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Description of the technical and organisational security measures implemented by the data importer in accordance with clause 4.1(d) and clause 5.1(c):

Firewalls, SSL, secure coding and development lifecycle, multi-factor authentication, data encryption, employee security training, and mobile device management including encryption, password policies, and lockout/wiping.

Corporate Customer

Signed: _____

Name: _____

Title: _____

Date: _____

Kandji, Inc.

Signed:  _____

Name: Mark Daughters

Title: Head of Operations

Date: 03/11/2020