Intapp Data Processing Addendum

This Data Processing Addendum ("Addendum") forms part of the Master Subscription and Services Agreement (the "Agreement") between: (i) Integration Appliance, Inc. and its Affiliates (collectively, "Intapp") and (ii) Customer and its Affiliates (collectively, "Customer"). Intapp's Affiliates may also enter into OSAs and SOWs with Customer, which OSAs and SOWs will be governed by the Agreement and in which event references in this Addendum to "Intapp" or "Integration Appliance, Inc." shall be deemed to be the Intapp Affiliate entering such OSA or SOW, including, where such Intapp Affiliate is a data importer, to its then current applicable address and other contact information.

The terms used in this Addendum shall have the meanings set forth in the Agreement unless otherwise provided. Except as modified below, the terms of the Agreement remain in effect.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement and apply to the processing of Customer Personal Data (as defined below) by Intapp. This Addendum shall not apply where and to the extent Intapp processes Personal Data (as defined below) as a Controller (as defined below). Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

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

1.1.1 **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, or that is a successor (whether by change of name, dissolution, merger, consolidation, reorganization, sale or other disposition) to any such business entity or its business and assets.

1.1.2 **"Applicable Laws"** means, with respect to any Customer Personal Data, European Union or Member State laws and the laws applicable in the United Kingdom (each as applicable).

1.1.3 "**Customer Personal Data**" means any Personal Data Processed by Intapp on behalf of the Customer as a Processor pursuant to or in connection with the Agreement in respect of which the Customer is subject to Data Protection Law; Customer Personal Data excludes Intapp CRM Data.

1.1.4 "**Data Protection Law**" means the California Consumer Privacy Act (CCPA), the UK Data Protection Law, the GDPR and laws implementing or supplementing the GDPR (each as applicable), as amended, replaced or superseded from time to time.

1.1.5 "**EEA**" means the European Economic Area.

1.1.6 "**EEA Standard Contractual Clauses**" means the EEA Controller to Processor SCCs and, if applicable, the EEA Processor to Controller SCCs.

1.1.7 "**EEA Controller to Processor SCCs**" means the relevant module of the Standard Contractual Clauses, for the transfer of personal data from a data exporter acting as a controller to a data importer acting as a processor, which is approved by the European Commission Implementing

Decision (EU) 2021/914 of 4 June 2021. A copy of the EEA Controller to Processor Clauses is set out at Appendix [2].

1.1.8 "**EEA Processor to Controller SCCs**" means the relevant module of the Standard Contractual Clauses, for the transfer of personal data from a data exporter acting as a processor to a data importer acting as a controller, which is approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021. If, applicable A copy of the EEA Processor to Controller Clauses is set out at Appendix [3].

1.1.9 "**EEA Processor to Processor SCCs**" means the relevant module of the Standard Contractual Clauses, for the transfer of personal data from a data exporter acting as a processor to a data importer acting as a processor, which is approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.1.10 "**GDPR**" means the EU General Data Protection Regulation 2016/679.

1.1.11 "**Intapp CRM Data**" means any data and information (including any personally identifiable information) provided or made available by Customer (including its employees, contractors agents and representatives) to Intapp which is required for Intapp's management of its relationship with Customer (including business contact information such as names, email addresses and telephone numbers).

1.1.12 **"Restricted Transfer**" means a transfer of Customer Personal Data:

(a) processed by a data exporter subject to the GDPR to a data importer not subject to the GDPR, ("**EEA Restricted Transfer**"); or

(b) from the UK to a jurisdiction outside the UK made by the Customer to Intapp ("**UK Restricted Transfer**"),

which transfer would be prohibited by the Data Protection Law that applies to the data exporter in the absence of a Transfer Mechanism. For the avoidance of doubt, if the data exporter exports personal data from the EEA or the United Kingdom, there will not be a Restricted Transfer where:

(a) the jurisdiction to which the personal data is transferred has been approved by the European Commission pursuant to Article 25(6) of the EC Directive 95/46 or Article 45 of the GDPR or, as applicable, an equivalent provision under UK Data Protection Law, as ensuring an adequate level of protection for the processing of personal data (an "**Adequate Country**"); or

(b) the transfer falls within the terms of a derogation as set out in Article 49 of the GDPR or the UK GDPR (as applicable);

(c) insofar as and to the extent that the GDPR applies to a particular transfer, the data importer falls within the territorial scope of application of the GDPR in accordance with Article 3 of the GDPR.

1.1.13 "**Services**" means, for the purposes of this Addendum, Services (as defined in the Agreement) as well as Support and Cloud Services (as applicable).

1.1.14 “**Standard Contractual Clauses**” means the EEA Standard Contractual Clauses and the UK Standard Contractual Clauses (each as applicable).

1.1.15 “**Subprocessor**” means any third party (including an Intapp Affiliate) appointed by or on behalf of Intapp to Process Customer Personal Data.

1.1.16 "**Transfer Mechanism**" means the Standard Contractual Clauses and/or any other means of effecting a Restricted Transfer which is permitted under the Data Protection Law including the GDPR that applies to the data exporter.

1.1.17 "**UK Data Protection Law**" means UK GDPR and the UK Data Protection Act 2018.

1.1.18 **"UK GDPR"** has the meaning defined in the UK Data Protection Act 2018.

1.1.19 "**UK Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission Decision C(2010) 593 ("**UK Controller to Processor SCCs**"), as amended, updated or replaced by the UK Government or the Information Commissioner's Office from time to time.

2. GDPR Terms

2.1 The Parties hereby agree that the terms and conditions set forth in Sections 2 through 11 and Section 13 only apply where the UK Data Protection Law and/or the GDPR govern the Processing of Personal Data (each as defined below) processed hereunder, and that for purposes of such Sections, the UK Data Protection Law and/or the GDPR (and laws implementing or supplementing the GDPR) shall be the applicable Data Protection Law.

2.2 The terms "**Commission”**, “**Controller**”, “**Data Subject**”, “**Member State**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing**”, "**Processor**" and "**Supervisory Authority**"have the same meaning as in in the GDPR. The terms **"data exporter"** and **"data importer"** have the meanings set out in the applicable Standard Contractual Clauses.

3. Processing of Customer Personal Data

3.1 This Addendum applies to Intapp’s Processing of Customer Personal Data in the course of Intapp providing Services to the Customer as a Processor. As such, for the purposes of the GDPR and UK GDPR, Intapp is the Processor and the Customer is the Controller.

3.2 Intapp will only Process Customer Personal Data in accordance with the Customer’s documented instructions unless Processing is required by Applicable Laws to which Intapp is subject, in which case Intapp will, to the extent permitted by Applicable Laws, inform the Customer of that legal requirement before Processing the Personal Data.

3.3 The Customer (i) instructs Intapp and (and authorises Intapp to instruct each Subprocessor) to Process Customer Personal Data, and in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement; and (ii) represents and warrants that (a) it is and will at all relevant times remain authorised to give such instructions, and (b) all such instructions comply with Applicable Laws.

3.4 Intapp will promptly notify the Customer if, in Intapp’s reasonable opinion, any instructions violate Applicable Laws.

3.5 Appendix 1 to this Addendum sets out certain information regarding Intapp’s Processing of the Customer Personal Data as required by Article 28(3) of the GDPR or equivalent provisions of any other applicable Data Protection Law (including the UK GDPR). Subject to the terms of, and the scope of

the Services agreed by the Parties in the Agreement, Customer may make reasonable amendments to Appendix 1 by written notice to Intapp from time to time as Customer reasonably considers necessary to meet those requirements.

3.6 Nothing in the Addendum shall prevent Intapp from processing Intapp CRM Data for its own purposes in its capacity as a Controller (subject to Intapp's compliance with Data Protection Law).

4. Intapp Personnel

Intapp will ensure that any Intapp employee, agent or contractor who may have access to the Customer Personal Data is subject to confidentiality undertakings in respect of the Customer Personal Data.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Intapp will implement appropriate technical and organisational measures in respect of Customer Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR or equivalent provisions of any other applicable Data Protection Law (including the UK GDPR).

5.2 In assessing the appropriate level of security, Intapp will take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

6.1 Customer authorises Intapp to appoint (and permit each Subprocessor appointed in accordance with this Clause 6 to appoint) Subprocessors in accordance with this Clause 6 and any restrictions in the Agreement.

6.2 Intapp may continue to use those Subprocessors it has engaged as at the date of this Addendum.

6.3 Intapp will post a notice of the appointment of any new Subprocessor, including details of the Processing to be undertaken by the Subprocessor, on its website. Provided that Customer subscribes to notifications from Intapp by emailing dpa@intapp.com, Customer will receive notice of such posting. If, within 10 business days of receiving the notice, Customer notifies Intapp in writing of any reasonable objections to the proposed appointment, Intapp will not appoint (or disclose any Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken.

6.4 With respect to each Subprocessor, Intapp will ensure that the arrangement between Intapp and the Subprocessor is governed by a written contract including terms offering at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR or equivalent provisions of any other applicable Data Protection Law (including the UK GDPR).

6.5 Intapp will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of any Subprocessor that cause Intapp to breach any of its obligations under this Addendum.

7. Data Subject Rights

7.1 The Services provide the Customer with a number of means by which the Customer may retrieve, correct, delete or restrict Customer Personal Data. Customer may use these means as technical and organizational measures to assist it in connection with its obligations under the applicable Data Protection Law, including its obligations relating to responding to requests from Data Subjects.

7.2 Intapp will (i) promptly notify Customer if it receives a request from a Data Subject under any applicable Data Protection Law in respect of Customer Personal Data; and (ii) not respond to that request except as required by Applicable Laws to which Intapp is subject, in which case Intapp will, to the extent permitted by Applicable Laws, inform Customer of that legal requirement before Intapp responds to the request.

8. Personal Data Breach

8.1 Intapp will notify Customer without undue delay, and in any event within 72 hours, upon becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under applicable Data Protection Law.

8.2 Intapp will cooperate with Customer and take such reasonable commercial steps as are appropriate in the circumstances to investigate, mitigate, and remediate each such Personal Data Breach.

9. Deletion or Return of Customer Personal Data

9.1 Subject to Clause 9.2, within 90 days of the expiration or termination of the Agreement (the "Termination Date"), Intapp will delete permanently the Customer Personal Data unless the Customer has previously deleted all such Customer Personal Data before the Termination Date.

9.2 Notwithstanding the foregoing, Intapp may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws (and Intapp may retain business contact information for Customer's staff); provided, however, that Intapp will ensure the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its retention, and for no other purpose.

10. Data Protection Impact Assessments and Audit Rights

10.1 Intapp will provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law (including the UK GDPR), in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, Intapp. The information made available in Clauses 10.2 through 10.4 is provided to assist the Customer in its compliance with those obligations.

10.2 Intapp is certified under ISO 27001 and agrees to maintain an information security program for the Services that complies with the ISO 27001 standards or such other alternative standards as are substantially equivalent to ISO 27001.

10.3 Intapp uses external auditors to verify the adequacy of its security measures. This audit (i) will be performed at least annually; (ii) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; and (iii) will be performed by

independent third-party security auditors. At the conclusion of the audit the auditor will prepare an audit report ("Report"). Upon the Customer's request, Intapp will provide Customer with the Report so that Customer can reasonably verify Intapp's compliance with its obligations under this Addendum. The Report will be deemed Intapp Confidential Information.

10.4 Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Intapp to carry out the audit described in Clause 10.3. If the Standard Contractual Clauses apply, nothing in this Clause 10 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

11. Restricted Transfers

11.1 The Parties will have in effect a Transfer Mechanism in respect of any Restricted Transfer.

11.2 Without prejudice to Clause 11.1, in the event of an EEA Restricted Transfer whereby Customer Personal Data is transferred from a data exporter acting as a controller to a data importer acting as a processor, the Parties shall comply with the EEA Controller to Processor SCCs.

11.3 Without prejudice to Clause 11.1 and Clause 11.2, in the event of an EEA Restricted Transfer whereby Customer Personal Data is transferred from a data exporter acting as a processor to a data importer acting as a controller, the Parties shall comply with the EEA Processor to Controller SCCs.

11.4 The Customer agrees that where Intapp engages a Subprocessor in accordance with Clause 6 for carrying out specific processing activities (on behalf of the Customer) and those processing activities involve a transfer of Customer Personal Data within the meaning of Chapter V of the GDPR, Intapp and Subprocessor can ensure compliance with Chapter V of the GDPR by using EEA Processor to Processor SCCs, provided the conditions for the use of those standard contractual clauses are met.

11.5 Without prejudice to Clause 11.1, in the event of a UK Restricted Transfer, the parties shall comply with the UK Controller to Processor SCCs.

11.6 Where any updates or amendments to, or replacement of, a Transfer Mechanism is approved by the competent authority/ies (including, where applicable, the European Commission, a UK Government Department or a competent regulatory authority) during the Term ("New Transfer Mechanism"), the New Transfer Mechanism will be deemed to replace the applicable Transfer Mechanism under this Addendum from the date on which Intapp issues notice to Customer and shall be deemed to take effect and be binding on the parties from the date stipulated in such notice.

11.7 For the avoidance of doubt, where this Schedule is intended to achieve compliance with a particular requirement of the applicable Transfer Mechanism, including the appendices required by the EEA Controller to Processor SCCs, the governing law in relation to that Transfer Mechanism shall be the law of the country where the data exporter is established.

12. CCPA Terms

12.1 The Parties hereby agree that the terms and conditions set forth in Sections 4, 5, 7, 8 , 9, 12, and 13only apply where the California Consumer Privacy Act, California Civil Code Sections 1798.100-1798.199 (as may be amended from time to time, the "**CCPA**") governs the processing of Personal Information (as defined below) processed hereunder, and that for purposes of such Sections, the CCPA shall be the applicable Data Protection Law.

12.2 The terms, "**Business**", "**Business Purpose**", "**Commercial Purpose**", "**Consumer**", "**Personal Information**", "**Sale**", "**Sell**", "**Selling**", and "**Service Provider**" have the same meaning as in the CCPA.

12.3 For the purposes of the CCPA, Customer is the Business and Intapp is the Service Provider.

12.4 For Customer Personal Information subject to the CCPA, Intapp acknowledges that it is prohibited from: (i) selling such Customer Personal Information; (ii) retaining, using, or disclosing such Customer Personal Information for a commercial purpose other than providing the Services or as otherwise permitted by the CCPA; and (iii) retaining, using, or disclosing such Customer Personal Information outside of the Agreement or other direct business relationship between Intapp and Customer; provided that (A) the foregoing shall not restrict Intapp's use of subcontractors or subprocessors in accordance with the Agreement and (B) nothing herein shall prevent Intapp from processing Intapp CRM Data for its own purposes in its capacity as a Business (subject to Intapp's compliance with Data Protection Law).

13. General Terms

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the UK Standard Contractual Clauses and clauses 17 (Governing Law) and 18 (Choice of forum and jurisdiction) of the EEA Standard Contractual Clauses:

13.1.1 the Parties agree to submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

13.2 In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses prevail. In the event of inconsistencies between this Addendum and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum prevail.

13.3 This Addendum remains in effect until termination or expiration of the Agreement.

13.4 The limitations of liability set out in the Agreement shall also apply to this Addendum such that the total, aggregate liability of Intapp under or in connection with this Addendum (including the Standard Contractual Clauses), together with all liability of Intapp under or in connection with the Agreement, shall be subject to the financial limitations and restrictions of liability set out in the Agreement.

13.5 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum will remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties" intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR or equivalent provisions of any other European Data Protection Law (including the GDPR).

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the Processing of Customer Personal Data

Intapp provides software and/or services designed to support Customer's management and execution of its internal business operations

The types of Customer Personal Data to be Processed

The Personal Data to be Processed by Intapp on behalf of Customer may include, but is not limited to the following categories of Personal Data:

- Names, contact details and other identification information
- Personal information
- Biographical and occupational information
- Employment and HR information

The categories of Data Subjects to whom the Customer Personal Data relates

The Personal Data to be Processed by Intapp on behalf of Customer may relate to, but is not limited to, the following categories of Data Subjects:

- Employees, workers, contractors, agents and volunteers
- Clients, customers and (where applicable) their personnel

The obligations and rights of Customer

The obligations and rights of the Customer are set out in the Agreement and this Addendum.

APPENDIX 2: EEA CONTROLLER TO PROCESSOR SCCs

(TRANSFER CONTROLLER-TO-PROCESSOR)

SECTION I

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) 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.A (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.A (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.B.

(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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) 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.B.

Clause 7

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.A.

(b) Once it has completed the Appendix and signed Annex I.A, 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.A.

(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.

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.B, 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.B. 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.B.

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 ([1]) (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 non-compliance. 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.

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least two weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object

(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. ([2]) 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

(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

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

the data exporter. 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.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.

(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

(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 sub-processor) 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

(a) *Where the data exporter is established in an EU Member State.* 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.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679. The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU)

2016/679. The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, 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

(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 ([3]);

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and

(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.

certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

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

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 minimisation

(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 of such noncompliance. 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(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 the Republic of Ireland.

(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

A. LIST OF PARTIES

Data exporter(s):

1.

Name: See Agreement

Address: See Agreement

Contact person's name, position and contact details: See Agreement

Activities relevant to the data transferred under these Clauses:

Signature and date: See Agreement

Role: Controller

Data importer(s):

1. Name: Integration Appliance, Inc.

Address: 3101 Park Blvd, Palo Alto, CA 94306

Contact person's name, position and contact details: See Agreement

Activities relevant to the data transferred under these Clauses:

Signature and date: See Agreement

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Employees, contractors, and agents of the
- Clients, customers and (where applicable) their personnel

Categories of personal data transferred

- Names, contact details and other identification information
- Personal Information
- Biographical and occupational information
- Employment and HR information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation,

access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- _____

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

- Frequently, if using a portion of the applicable Intapp Product that is provided by a sub-processor outside of the EEA, as detailed at www.intapp.com/sub-processors/
- Occasionally, depending on the amount of Support requests from the Data Exporter.
- Rarely, as necessary for the Data Importer to fulfill its security and availability commitments

Nature of the processing

- Depends on the processing taking place, for transfers necessitated by use of Products provided by Subprocessors the nature of the processing could include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

Purpose(s) of the data transfer and further processing

- Provision of the Cloud Service, as outlined in the Agreement and applicable OSA and SOW (as these terms are defined in the Agreement).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- Until the termination or expiration of the applicable OSA plus 180 days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- Same as above

C. COMPETENT SUPERVISORY AUTHORITY

The Data Protection Commission of the Republic of Ireland.

ANNEX II

SECURITY PRINCIPLE AND CRITERIA TABLE

The following controls may be modified from time to time as appropriate to provide an equal or better level of security:

Control #	Control Activity Specified by Intapp
CONTROL ENVIRONMENT	
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	Documented policies and procedures are in place to guide personnel in the entity's security, availability, and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.
CC1.1.2	Employees are required to sign and acknowledge a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
CC1.1.3	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC1.1.4	Employment candidates undergo a background screening as a component of the hire process.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	The board of directors establishes and maintains a formal charter and set of bylaws which describes their responsibilities and oversight of management's system of internal control.
CC1.2.2	The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
CC1.2.3	Board of directors and committee meetings are held on at least a quarterly basis to review internal control performance.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.
CC1.3.2	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
CC1.3.3	Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the security committee.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	New employee hiring documentation is in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
CC1.4.2	Employment candidates undergo a background screening as a component of the hire process.
CC1.4.3	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC1.4.4	Employees are required to complete security awareness training at least annually.
CC1.4.5	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.

CC.1.4.6	Personnel are evaluated on an annual basis to ensure that they have the skills and knowledge to perform their job responsibilities.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	Responsibility for controls is clearly assigned to roles in the organization through documented procedures.
CC1.5.2	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
CC1.5.3	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC1.5.4	Personnel are evaluated on an annual basis to ensure that they have the skills and knowledge to perform their job responsibilities.
COMMUNICATION AND INFORMATION	
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	An information security policy is formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.
CC2.1.2	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC2.1.3	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC2.1.4	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.
CC2.1.5	Management reviews audit reports from third-party service providers on an annual basis to help ensure compliance with security, availability and confidentiality commitments and system requirements.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	Documented policies and procedures are in place to guide personnel in the entity's security, availability, and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.
CC2.2.2	Employees are required to acknowledge their security responsibilities upon hire and on an annual basis thereafter.
CC2.2.3	Documented job descriptions are in place to establish and define the structure, reporting lines, and authorities and responsibilities for employment positions.
CC2.2.4	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC2.2.5	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.
CC2.2.6	Employees are required to sign and acknowledge a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
CC.2.2.7	Security committee meetings are held on a quarterly basis to discuss ongoing objectives and their effect on the system.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.
CC2.3.2	The entity's security, availability, and confidentiality commitments and the associated system requirements are documented in customer contracts and on the company website.

CC2.3.3	Customer notifications are provided using the cloud services status webpage.
RISK ASSESSMENT	
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.
CC3.1.2	Management formally documents and reviews the company's security objectives to help ensure they align with the company's mission and are utilized as part of the annual risk assessment process.
CC3.1.3	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.
CC3.2.2	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.2.3	The risk assessment includes the analysis of potential threats and vulnerabilities introduced from doing business with vendors and business partners.
CC3.2.4	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis and results are included in the risk assessment, and remediation plans are proposed and tracked through resolution.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.
CC3.3.2	A formal risk assessment is performed on an annual basis that considers the potential for fraud. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	A formal risk assessment is performed on an annual basis that considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.
CC3.4.2	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.
CC3.4.3	Management reviews audit reports from third-party service providers on an annual basis to help ensure compliance with security, availability and confidentiality commitments and system requirements.
CC3.4.4	Security committee meetings are held on a quarterly basis to discuss ongoing objectives and their effect on the system.
MONITORING ACTIVITIES	
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC4.1.2	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.

CC4.1.3	Management reviews audit reports from third-party service providers on an annual basis to help ensure controls are operating effectively and any identified risks are addressed.
CC4.1.4	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC4.1.5	Monitoring applications are utilized to monitor system performance and are configured to send automated alerts to DevOps personnel when predefined thresholds have been exceeded.
CC4.1.6	An internal compliance assessment is completed on a semi-annual basis. The assessment results are documented and reviewed by management.
CC4.1.7	Management compiles and provides internal control performance metrics to the security committee on a quarterly basis. These metrics are formally documented in the internal control performance dashboard for committee review.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
CC4.2.1	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC4.2.2	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC4.2.3	Management compiles and provides internal control performance metrics to the security committee on a quarterly basis. These metrics are formally documented in the internal control performance dashboard for committee review.
CONTROL ACTIVITIES	
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security, availability, and confidentiality of data and service.
CC5.1.2	A formal risk assessment is performed on an annual basis to assess the potential risks, vulnerabilities, and control activities related to the security, availability, and confidentiality of data and service.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	Control activities over technology are identified as part of the annual risk assessment process to support the achievement of objectives and are documented within the risk assessment report.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	Documented policies and procedures are in place to guide personnel in the entity's security, availability, and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.
CC5.3.2	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC5.3.3	Employees are required to complete security awareness at least annually.
LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
CC6.1.1	Production system user access requests are documented in a ticket and require the approval of management.

CC6.1.2	The in-scope systems are configured to authenticate users with unique user credentials and enforce predefined user account and minimum password requirements or SSH private key authentication.
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.
CC6.1.5	The in-scope systems are configured to enforce multi-factor authentication to access the production environment.
CC6.1.6	A log monitoring system is utilized to monitor and log events for certain in-scope systems that include, but are not limited to, the following: · Account management · Logon events · Policy change · Privileged use
CC6.1.7	Employees are required to acknowledge their security responsibilities upon hire and on an annual basis thereafter.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.2.1	Production system user access requests are documented in a ticket and require the approval of management.
CC6.2.2	System access to the in-scope production systems is revoked upon termination of employment.
CC6.2.3	User access reviews are performed on an annual basis to ensure that access to data is restricted.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	Production system user access requests are documented in a ticket and require the approval of management.
CC6.3.2	The in-scope systems are configured to authenticate users with unique user credentials and enforce predefined user account and minimum password requirements or SSH private key authentication.
CC6.3.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.
CC6.3.5	User access reviews are performed on an annual basis to ensure that access to data is restricted.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
	AWS and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.

CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
	AWS and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.
CC6.6.2	Security groups and NSGs acting as a firewall system are in place to restrict inbound and outbound traffic.
CC6.6.3	Security personnel review the security group and NSG rulesets on at least an annual basis.
CC6.6.4	Web servers utilize transport layer security (TLS) encryption for web communications.
CC6.6.5	Encrypted VPNs are required for remote access to production and enforce username and password for authentication.
CC6.6.6	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC6.6.7	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC6.6.8	An intrusion detection system (IDS) is utilized to analyze and report network events and to block suspected or actual network security breaches.
CC6.6.9	Security monitoring tools are configured to alert SOC team for possible or actual security breaches.
CC6.6.10	Production databases are configured to encrypt data at rest.
	AWS and Microsoft Azure are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Intapp OnePlace and DealCloud Platform systems reside.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.
CC6.7.2	Web servers utilize TLS encryption for web communications.
CC6.7.3	Encrypted VPNs are required for remote access to production and enforce username and password for authentication.
CC6.7.4	The automated backup systems are configured to encrypt backup media.
	AWS and Microsoft Azure are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Intapp OnePlace and DealCloud systems reside.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC6.8.1	Cloud-based endpoint protection software is configured to protect registered production servers and workstations in real-time.
CC6.8.2	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC6.8.3	File integrity monitoring tool is in place to monitor, detect, and alert upon unauthorized software installation or configuration changes to certain production systems.
SYSTEM OPERATIONS	

CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
	AWS and Microsoft Azure are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where Intapp OnePlace and DealCloud systems reside.
CC7.1.1	The DevOps team has formally documented standard build procedures for installation and maintenance of production servers.
CC7.1.2	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC7.1.3	Annual penetration testing is performed by a third-party vendor, and remediation plans are proposed and tracked through resolution.
CC7.1.4	Security personnel review the security group and NSG rulesets on at least an annual basis.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
	AWS and Microsoft Azure are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where Intapp OnePlace and DealCloud systems reside.
CC7.2.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.2.2	A log monitoring system is utilized to monitor and log events for certain in-scope systems that include, but are not limited to, the following: • Account management • Logon events • Policy change • Privileged use
CC7.2.3	Monitoring applications are utilized to monitor system performance and are configured to send automated alerts to DevOps personnel when predefined thresholds have been exceeded.
CC7.2.4	Vulnerability assessments are performed by Intapp SOC personnel on a quarterly basis to identify the functionality of control activities, and remediation plans are proposed and tracked through resolution.
CC7.2.5	An IDS is utilized to analyze and report network events and to block suspected or actual network security breaches.
CC7.2.6	Security monitoring tools are configured to alert SOC team for possible or actual security breaches.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.3.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.3.2	Automated and manual systems are utilized to document and track security incidents and remediation activities.
CC7.3.3	Incidents requiring a change to the system follow the standard change control process.
CC7.3.4	An IDS is utilized to analyze and report network events and to block suspected or actual network security breaches.
CC7.3.5	Security monitoring tools are configured to alert SOC team for possible or actual security breaches.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	

CC7.4.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.4.2	Automated and manual systems are utilized to document and track security incidents and remediation activities.
CC7.4.3	Security committee meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.5.2	Automated and manual systems are utilized to document and track incidents and remediation activities.
CC7.5.3	Security committee meetings are held on a quarterly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.
CHANGE MANAGEMENT	
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CC8.1.1	Change management policies and procedures are in place to guide personnel in change management procedures through the change lifecycle.
CC8.1.2	A change management meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.
CC8.1.3	A change tracking system is in place to centrally document, manage, and monitor changes from change requests through implementation.
CC8.1.4	Changes are authorized, peer reviewed, tested, and approved prior to implementation.
CC8.1.5	Development and test environments are logically separated from the production environment.
CC8.1.6	Version control software is utilized to restrict access to application source code and provide rollback capabilities.
CC8.1.7	The version control software is configured to restrict users from merging or deploying code without secondary approval.
CC8.1.8	The ability to modify application source code is restricted to user accounts accessible by authorized personnel.
CC8.1.9	The ability to implement changes into the production environment is restricted to user accounts accessible by authorized non-development personnel.
CC8.1.10	Administrative access privileges within the version control software are restricted to user accounts accessible by authorized personnel.
CC8.1.11	Client data is not utilized for application change control development or testing.
CC8.1.12	File integrity monitoring tool is in place to monitor, detect, and alert upon unauthorized software installation or configuration changes to certain production systems.
RISK MITIGATION	
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security, availability, and confidentiality of data and service.
CC9.1.2	A formal risk assessment is performed on an annual basis that considers potential business disruptions. Risks that are identified are formally documented for management review and includes the objectives and associated risks that address the security, confidentiality, integrity, and availability of the in-scope systems.

CC9.1.3	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
CC9.1.4	Risk mitigation activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	A vendor management policy is in place that addresses the following: • Due diligence process prior to accepting new vendors or business partners • Monitoring process to review vendor and business partner compliance on a periodic basis • Termination of contracts
CC9.2.2	Confidentiality agreements are required to be in place with third parties prior to sharing information designated as confidential.
CC9.2.3	Management reviews audit reports from third-party service providers on an annual basis to help ensure compliance with security, availability and confidentiality commitments and system requirements.

Additional Criteria for Availability

Control #	Control Activity Specified by Intapp
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	
	AWS and Microsoft Azure are responsible for ensuring capacity demand controls are in place to meet Intapp's availability commitments and requirements.
A1.1.1	Monitoring applications are utilized to monitor system performance and are configured to send automated alerts to DevOps personnel when predefined thresholds have been exceeded.
A1.1.2	Security committee meetings are held on a quarterly basis to review availability trends.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	
	AWS and Microsoft Azure are responsible for ensuring environmental protection controls are in place to meet Intapp's availability commitments and requirements.
A1.2.1	An automated backup system is in place to perform scheduled backups of production databases on a daily basis.
A1.2.2	The automated backup system is configured to replicate production databases to multiple regions.
A1.2.2	The automated backup system is configured to notify DevOps personnel regarding the failure of backup jobs.
A1.2.3	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
A1.3.1	DevOps personnel perform restorations from backup files as a component of standard business operations.
A1.3.2	A disaster recovery plan exercise is performed and tested on an annual basis.

Additional Criteria for Confidentiality

Control #	Control Activity Specified by Intapp
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	

C1.1.1	The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts and on the company website.
C1.1.2	Documented data retention policies are in place to guide personnel on the procedures for retention of customer data.
C1.1.3	Product management reviews the retention of customer data on an annual basis to verify that customer data is retained in accordance with data retention commitments.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	
C1.2.1	The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts and on the company website.
C1.2.2	Documented disposal policies are in place to guide personnel on the procedures for disposal of customer data.
C1.2.3	Product management reviews the disposal of customer data on an annual basis to verify that customer data is disposed of in accordance with data disposal commitments.
C1.2.4	A customer data destruction ticket is completed to track the disposal of customer data upon termination of the services in accordance with the documented data disposal commitments.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

- See www.intapp.com/sub-processors