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 "Customer" (as defined in the Agreement).

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 by Intapp. This Addendum shall not apply where and to the extent Intapp processes Personal Data as a Controller. 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, (a) during the Brexit Transition Period: European Union or Member State laws (or, in relation to Processing which is exclusively subject to the laws of United Kingdom, the laws applicable in the United Kingdom) and (b) with effect from the end of the Brexit Transition Period: European Union or Member State laws and the laws applicable in the United Kingdom (each as applicable).

1.1.3 **Brexit Transition Period** means the period which began at 11 pm (UK time) on 31 January 2020 and ends on IP completion day as defined in s.39 of the European Union (Withdrawal Agreement) Act 2020.

1.1.4 "**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.

1.1.5 "**European Data Protection Law**" means the GDPR, the UK GDPR and laws implementing or supplementing the GDPR, as amended, replaced or superseded from time to time.

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

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

1.1.8 "**Intapp CRM Data**" means any data and information (including any personally identifable 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).

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

(a) the EEA to a jurisdiction outside the EEA made by the Customer to Intapp, which transfer would be prohibited by European Data Protection Law in the absence of a Transfer Mechanism; or

(b) (with effect from the end of the Brexit Transition Period) the UK to a jurisdiction outside the UK made by the Customer to Intapp which transfer would be prohibited by European Data Protection Law in the absence of a Transfer Mechanism.

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

1.1.11 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, which are incorporated into and made part of this Addendum.

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

1.1.13 "**Transfer Mechanism**" means the Standard Contractual Clauses and/or any other means of effecting a Restricted Transfer which is permitted under the law of the Customer.

1.1.14 **"UK GDPR"** means, with effect from the end of the Brexit Transition Period, the GDPR as implemented in the UK.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" have the same meaning as in the European Data Protection Law.

2. Processing of Customer Personal Data

2.1 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, Intapp is the Processor and the Customer is the Controller.

2.2 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.

2.3 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.

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

2.5 Annex 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 European Data Protection Law (including the UK GDPR). Customer may make reasonable amendments to Annex 1 by written notice to Intapp from time to time as Customer reasonably considers necessary to meet those requirements.

2.6 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 European Data Protection Law).

3. 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.

4. Security

4.1 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 European Data Protection Law (including the UK GDPR).

4.2 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.

5. Subprocessing

5.1 Customer authorises Intapp to appoint (and permit each Subprocessor appointed in accordance with this Clause 5 to appoint) Subprocessors in accordance with this Clause 5 and any restrictions in the Agreement.

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

5.3 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, 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.

5.4 With respect to each Subprocessor, Intapp will:

5.4.1 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 European Data Protection Law (including the UK GDPR); and

5.4.2 If that arrangement involves a Restricted Transfer, ensure that at all relevant times a Transfer Mechanism is in place between Intapp and the Subprocessor, or before the Subprocessor first Processes Customer Personal Data, procure that it has a Transfer Mechanism with the Customer.

5.5 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.

6. Data Subject Rights

6.1 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 European Data Protection Law, including its obligations relating to responding to requests from Data Subjects.

6.2 Intapp will (i) promptly notify Customer if it receives a request from a Data Subject under any European 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.

7. Personal Data Breach

7.1 Intapp will notify Customer without undue delay 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 the European Data Protection Law.

7.2 Intapp will cooperate with Customer and take such reasonable commercial steps as requested by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Deletion or Return of Customer Personal Data

8.1 Subject to Clause 8.2, 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.

8.2 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.

9. Data Protection Impact Assessments and Audit Rights

9.1 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 European 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 9.2 through 9.4 is provided to assist the Customer in its compliance with those obligations.

9.2 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.

9.3 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.

9.4 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 9.3. If the Standard Contractual Clauses apply, nothing in this Clause 9 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

10. Restricted Transfers

10.1 Intapp will have in effect a Transfer Mechanism in respect of any Restricted Transfer.

11. General Terms

11.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

11.1.1 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

11.1.2 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.

11.2 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.

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

11.4 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.

11.5 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.

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 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.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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

Name of the data exporting organisation: **Customer**

Address: **Customer's address provided in the Agreement**

Tel.: _____;
fax: _____;
e-mail: _____

Other information needed to identify the organisation

.....
(the data **exporter**)

And

Name of the data importing organisation: **Integration Appliance, Inc.**

Address: 200 Portage Ave,
Palo Alto, CA 94306
US

Tel.: +1 650 852 0400

fax: +1 650 852 0402

e-mail: legal@intapp.com

Other information needed to identify the organisation:

Integration Appliance, Inc.
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

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

(b) "*the data exporter"* means the controller who transfers the personal data;

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

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

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

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

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular

where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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

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

enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

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

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

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

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

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

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter: Customer
Name (written out in full): **Provided in the Agreement**
Position: **Provided in the Agreement**
Address: **Provided in the Agreement**

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

On behalf of the data importer: Integration Appliance, Inc.
Name (written out in full): **Provided in the Agreement**
Position: **Provided in the Agreement**
Address: 200 Portage Ave,
Palo Alto,
CA 94306,
US

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is:

Customer

Data importer
The data importer is:

Integration Appliance, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:
Categories may include, but are not limited to:

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

Categories of data
The personal data transferred concern the following categories of data:
Categories may include, but are not limited to:

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

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

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

See Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

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 the Service Organization
CC1.0: Common Criteria Related to Organization and Management	
CC1.1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	
CC1.1.1	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.
CC1.1.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for information security employees.
CC1.2: Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity"s system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC1.2.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for information security.
CC1.2.2	Responsibility for controls is clearly assigned to appropriate roles in the organization through documented procedures.
CC1.3: The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.	
CC1.3.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for information security employees.
CC1.3.2	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.
CC1.3.3	Employees are required to complete security awareness training upon hire and at least annually.
CC1.3.4	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC1.3.5	Personnel are evaluated to ensure that they have the skills and knowledge to perform their duties.
CC1.4: The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	
CC1.4.1	Employment candidates undergo a background check as a component of the hiring process.
CC1.4.2	All employees are required to sign an acknowledgement of their security responsibilities upon hire and on an annual basis thereafter.

Control #	Control Activity Specified by the Service Organization
CC1.4.3	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC2.0: Common Criteria Related to Communications	
CC2.1: Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	
CC2.1.1	A system description is documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems and is communicated to authorized internal and external users.
CC2.2: The entity"s security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	
CC2.2.1	The entity"s security, availability, and confidentiality commitments and the associated system requirements are documented in customer contracts.
CC2.2.2	Documented policies and procedures are in place to govern the provision for training and other resources to support system security policies.
CC2.2.3	Documented policies and procedures are in place to guide personnel in the entity"s security and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel.
CC2.2.4	All employees are required to sign an acknowledgement of their security responsibilities upon hire and on an annual basis thereafter.
CC2.2.5	Employees are required to complete security awareness training upon hire and at least annually.
CC2.3: The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	
CC2.3.1	Documented policies and procedures are in place to guide personnel in the entity"s security and confidentiality commitments and the associated system requirements. The policies and procedures are communicated to internal personnel.
CC2.3.2	Application documentation is made available to guide customers on the proper and secure use of the system.
CC2.3.3	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC2.3.4	The entity"s security, availability, and confidentiality commitments and the associated system requirements are documented in customer contracts.
CC2.3.5	Documented policies and procedures are in place to govern the provision for training and other resources to support system security policies.
CC2.3.6	All employees are required to sign an acknowledgement of their security responsibilities upon hire and on an annual basis thereafter.
CC2.4: Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.	
CC2.4.1	Documented policies and procedures are in place to govern the provision for training and other resources to support system security policies.
CC2.4.2	All employees are required to sign an acknowledgement of their security responsibilities upon hire and on an annual basis thereafter.
CC2.4.3	Employees are required to complete security awareness training upon hire and at least annually.
CC2.4.4	The entity"s security, availability, and confidentiality commitments and the associated system requirements are documented in customer contracts.

Control #	Control Activity Specified by the Service Organization
CC2.5: Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	
CC2.5.1	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC2.6: System changes that affect internal and external users" responsibilities or the entity"s commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.	
CC2.6.1	Customer notifications are provided using the Intapp Maintenance webpage.
CC2.6.2	Development team meetings are held weekly to discuss upcoming project and application changes.
CC2.6.3	Release notes are documented and communicated to customers and implementation, QA, and service assurance management personnel for changes and maintenance that affect system security.
CC2.6.4	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for information security employees.
CC2.6.5	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.
CC3.0: Common Criteria Related to Risk Management and Design and Implementation of Controls	
CC3.1: The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	
CC3.1.1	An inventory of in-scope systems is maintained and reviewed on at least an annual basis during the risk assessment process.
CC3.1.2	Documented policies and procedures are in place to guide personnel when performing the risk assessment process that includes identifying and understanding the assets and the associated risks.
CC3.1.3	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.
CC3.1.4	The information security team monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by the information security team as part of the annual risk assessment and information security planning process.
CC3.2: The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	
CC3.2.1	Security reviews and vulnerability assessments are performed by information technology personnel and third party vendors on a periodic basis. Remediation plans are proposed and monitored through resolution.
CC3.2.2	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. The security monitoring applications are configured to provide e-mail alerts to Intapp personnel when suspicious activity is detected.
CC3.2.3	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.
CC3.2.4	The information security team monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by the information security team as part of the annual risk assessment and information security planning process.

Control #	Control Activity Specified by the Service Organization
CC4.0: Common Criteria Related to Monitoring Controls	
CC4.1: The design and operating effectiveness of controls are periodically evaluated against the entity"s commitments and system requirements as they relate to security, availability, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	
CC4.1.1	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.
CC4.1.2	Security reviews and vulnerability assessments are performed by information technology personnel and third party vendors on a periodic basis. Remediation plans are proposed and monitored through resolution.
CC4.1.3	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. The security monitoring applications are configured to provide e-mail alerts to Intapp personnel when suspicious activity is detected.
CC5.0: Common Criteria Related to Logical and Physical Access Controls	
CC5.1: Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC5.1.1	Documented information security policies and procedures are in place to guide personnel in security practices that include, but not limited to, the following: • Access control • Password requirements • Internet usage • Acceptable use
CC5.1.2	Production system user access requests are documented in a ticket and require the approval of management.
CC5.1.3	System access to the in-scope production systems is revoked upon termination of employment.
CC5.1.4	User access reviews are performed on a quarterly basis to ensure that access to data was restricted.
CC5.1.5	The in-scope systems are configured to authenticate users with a unique user account and password before being granted access to the production environment. Password parameters are configured to enforce the following password requirements: • Minimum password length • Password complexity requirements
CC5.1.6	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.
CC5.1.7	Multi-factor authentication (MFA) based on login credentials and a time-based token is utilized before granting access to AWS production.
CC5.1.8	Encrypted VPNs are required for remote access to the Time Cloud production systems.
CC5.1.9	The production servers are configured to log access related events. Logs are reviewed by DevOps personnel on an ad-hoc basis.
CC5.1.10	End users are required to authenticate to Intapp Time Cloud, Intapp Open Cloud, and Intapp Flow Cloud applications via user accounts and password.
CC5.1.11	Web servers utilize transport layer security (TLS) encryption for web communication sessions.
CC5.1.12	Security reviews and vulnerability assessments are performed by information technology personnel and third party vendors on a periodic basis. Remediation plans are proposed and monitored through resolution.

Control #	Control Activity Specified by the Service Organization
CC5.1.13	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. The security monitoring applications are configured to provide e-mail alerts to Intapp personnel when suspicious activity is detected.
AWS and UKFast are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Intapp systems reside.	
CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC5.2.1	Production system user access requests are documented in a ticket and require the approval of management.
CC5.2.2	MFA based on login credentials and a time-based token is utilized before granting access to AWS production.
CC5.2.3	System access to the in-scope production systems is revoked upon termination of employment.
CC5.2.4	User access reviews are performed on a quarterly basis to ensure that access to data was restricted.
AWS and UKFast are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Intapp systems reside.	
CC5.3: Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC5.3.1	The in-scope systems are configured to authenticate users with a unique user account and password before being granted access to the production environment. Password parameters are configured to enforce the following password requirements: • Minimum password length • Password complexity requirements
CC5.3.2	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.
CC5.3.3	MFA based on login credentials and a time-based token is utilized before granting access to AWS production.
AWS and UKFast are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Intapp systems reside.	
CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC5.4.1	Production system user access requests are documented in a ticket and require the approval of management.
CC5.4.2	System access to the in-scope production systems is revoked upon termination of employment.
CC5.4.3	User access reviews are performed on a quarterly basis to ensure that access to data was restricted.
CC5.4.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.

Control #	Control Activity Specified by the Service Organization
AWS and UKFast are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Intapp systems reside.	
CC5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
AWS and UKFast are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	
CC5.6: Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity"s commitments and system requirements.	
CC5.6.1	AWS security groups are defined on in-scope systems to filter unauthorized inbound network traffic from the Internet.
CC5.6.2	A firewall system is in place to filter unauthorized inbound network traffic from the Internet to in-scope production systems. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
CC5.6.4	Web servers utilize TLS encryption for web communication sessions.
CC5.6.5	Encrypted VPNs are required for remote access to the Intapp Time Cloud production systems.
CC5.6.6	MFA based on login credentials and a time-based token is utilized before granting access to AWS production.
CC5.6.7	Firewall rules shall be reviewed for security and appropriateness on a periodic and at least semi-annual basis.
CC5.6.8	Security reviews and vulnerability assessments are performed by information technology personnel and third party vendors on a periodic basis. Remediation plans are proposed and monitored through resolution.
CC5.6.9	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. The security monitoring applications are configured to provide e-mail alerts to Intapp personnel when suspicious activity is detected.
AWS and UKFast are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Intapp systems reside.	
CC5.7: The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	
CC5.7.1	AWS security groups are defined on in-scope systems to filter unauthorized inbound network traffic from the Internet.
CC5.7.2	A firewall system is in place to filter unauthorized inbound network traffic from the Internet to in-scope production systems. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
CC5.7.3	Web servers utilize TLS encryption for web communication sessions.
CC5.7.4	Encrypted VPNs are required for remote access to the Intapp Time Cloud production systems.
CC5.7.5	MFA based on login credentials and a time-based token is utilized before granting access to AWS production.
AWS and UKFast are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Intapp systems reside.	
CC5.8: Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC5.8.1	Intapp uses anti-virus software to scan code changes prior to implementation to protect against infection by computer viruses and malicious code.
CC5.8.2	A central antivirus server is configured with antivirus software to protect registered Intapp Time Cloud production systems.

Control #	Control Activity Specified by the Service Organization
CC6.0: Common Criteria Related to System Operations	
CC6.1: Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC6.1.1	Security reviews and vulnerability assessments are performed by information technology personnel and third party vendors on a periodic basis. Remediation plans are proposed and monitored through resolution.
CC6.1.2	The production servers are configured to log access related events. Logs are reviewed by DevOps personnel on an ad-hoc basis.
CC6.1.3	Automated backup systems are in place to perform scheduled backups of production servers at predefined times.
CC6.1.4	The production systems are configured to failover to a separate availability zone in the event of system failure or outage.
CC6.2: Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity"s commitments and system requirements.	
CC6.2.1	All employees are required to sign an acknowledgement of their responsibilities for security on an annual basis.
CC6.2.2	Documented escalation procedures for reporting security, availability, or confidentiality incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
CC6.2.3	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
CC6.2.4	Periodically and at least annually the incident response program shall be tested. Any findings are documented and tracked to closure.
CC7.0: Common Criteria Related to Change Management	
CC7.1: The entity"s commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	
CC.7.1.1	Documented policies and procedures are in place to guide personnel in the in-scope systems change management process.
CC7.1.2	A change management meeting is held on an as needed basis to discuss and communicate the ongoing and upcoming projects that affect the system.
CC7.1.3	A change management ticketing system is utilized to log and track in-scope system change information.
CC7.1.4	Changes made to in-scope systems are authorized, tested, and approved prior to implementation.
CC7.1.5	Development and test environments are logically separated from the production environment.
CC7.1.6	Access privileges to make changes to production is restricted to authorized personnel.
CC7.1.7	Security incidents requiring a change to the system follow the standard change control process.
CC7.2: Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC7.2.1	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.
CC7.2.2	The information security team monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by the information security team as part of the annual risk assessment and information security planning process.
CC7.2.3	Changes made to in-scope systems are authorized, tested, and approved prior to implementation.

Control #	Control Activity Specified by the Service Organization
CC7.3: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity"s commitments and system requirements as they relate to security, availability, and confidentiality.	
CC7.3.1	Security reviews and vulnerability assessments are performed by information technology personnel and third party vendors on a periodic basis. Remediation plans are proposed and monitored through resolution.
CC7.3.2	Security incidents requiring a change to the system follow the standard change control process.
CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity"s security, availability, and confidentiality commitments and system requirements.	
CC7.4.1	Access privileges to promote changes into the production environment are restricted to user accounts accessible by authorized personnel segregated from individuals with development responsibility for Intapp Time Cloud production systems.
CC7.4.2	AWS monitors changes to Intapp Open Cloud and Intapp Flow Cloud environments and notifies personnel outside of the DevOps team for any production system changes.
CC7.4.3	Changes made to in-scope systems are authorized, tested, and approved prior to implementation.
CC7.4.4	Development and test environments are logically separated from the production environment.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization
A1.1: Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity"s availability commitments and system requirements.	
A1.1.1	Enterprise monitoring applications are utilized to monitor the in-scope systems and alert DevOps personnel when predefined thresholds have been met.
A1.1.2	The production servers are configured to log access related events. Logs are reviewed by DevOps personnel on an ad-hoc basis.
A1.1.3	The DevOps team monitors availability trends and availability on an ongoing basis to ensure system commitments are met.
A1.1.4	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.
A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity"s availability commitments and system requirements.	
A1.2	Automated backup systems are in place to perform scheduled backups of production servers at predefined times.
A1.2	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
A1.2	The production systems are configured to failover to a separate availability zone in the event of system failure or outage.
A1.2	Enterprise monitoring applications are utilized to monitor the in-scope systems and alert DevOps personnel when predefined thresholds have been met.
AWS and UKFast are responsible for designing, developing, implementing, operating, maintaining and monitoring controls to protect against physical and environmental factors.	
A1.3: Recovery plan procedures supporting system recovery are tested to help meet the entity"s availability commitments and system requirements.	

Control #	Control Activity Specified by the Service Organization
A1.3.1	Automated backup systems are in place to perform scheduled backups of production servers at predefined times.
A1.3.2	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
A1.3.3	The business continuity plan shall be tested on at least an annual basis.
AWS and UKFast are responsible for managing the redundant infrastructure utilized and configured by Intapp for recovery operations of Intapp Cloud.	

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization
C1.1: Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity"s confidentiality commitments and system requirements.	
C1.1.1	Client data is not utilized for application change control development or testing.
C1.2: Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity"s confidentiality commitments and system requirements.	
C1.2.1	Intapp implements and maintains data segregation between each Customer's data to ensure the confidentiality of that data.
C1.2.2	Sensitive data is stored in an encrypted format where feasible with access to the cryptographic keys restricted to authorized individuals.
C1.2.3	MFA based on login credentials and a time-based token is utilized before granting access to AWS production.
C1.2.4	The in-scope systems are configured to authenticate users with a unique user account and password before being granted access to the production environment. Password parameters are configured to enforce the following password requirements: • Minimum password length • Password complexity requirements
C1.2.5	Encrypted VPNs are required for remote access to the Intapp Time Cloud production systems.
C1.2.6	End users are required to authenticate to Intapp Time Cloud, Intapp Open Cloud, and Intapp Flow Cloud applications via user accounts and password.
C1.3: Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity"s confidentiality commitments and system requirements.	
C1.3.1	MFA based on login credentials and a time-based token is utilized before granting access to AWS production.
C1.3.2	The in-scope systems are configured to authenticate users with a unique user account and password before being granted access to the production environment. Password parameters are configured to enforce the following password requirements: • Minimum password length • Password complexity requirements
C1.3.3	Encrypted VPNs are required for remote access to the Intapp Time Cloud production systems.
C1.3.4	End users are required to authenticate to Intapp Time Cloud, Intapp Open Cloud, and Intapp Flow Cloud applications via user accounts and password.

Control #	Control Activity Specified by the Service Organization
C1.4: The entity obtains confidentiality commitments that are consistent with the entity"s confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	
C1.4.1	The entity"s confidentiality commitments and requirements are documented in customer contracts. The contracts are updated and a signature is obtained should the confidentiality practice change.
C1.5: Compliance with the entity"s confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	
C1.5.1	Intapp does not transfer client data to any third party outside the services context. Intapp Cloud data resides on servers in AWS and the UKFast datacenter facility; however, employees of those providers do not have access to customer data.
C1.6: Changes to the entity"s confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	
C1.6.1	The entity"s confidentiality commitments and requirements are documented in customer contracts. The contracts are updated and a signature is obtained should the confidentiality practice change.
C1.7: The entity retains confidential information to meet the entity"s confidentiality commitments and system requirements.	
C1.7.1	Documented policies and procedures are in place to guide personnel in the retention of client data.
C1.7.2	Client data is retained in accordance with the client contracts.
C1.8: The entity disposes of confidential information to meet the entity"s confidentiality commitments and system requirements.	
C1.8.1	Documented policies and procedures are in place to guide personnel in the deletion of client data.
C1.8.2	IT personnel dispose of customer data upon termination in accordance with client contracts and documented policies and procedures.