1 January 2023

iManage Cloud Services Agreement

This iManage Cloud Services Agreement was certified to be **more customer-favorable than 89% of 1,000+ similar agreements reviewed by TermScout, as of 1 January 2023.*

This iManage Cloud Services Agreement (this "**Agreement**"), is by and between the iManage entity described in **Section 12.13** below ("**iManage**"), and the customer identified in the applicable Order ("**Customer**"). iManage and Customer are sometimes referred to herein individually as a "**Party**" and together as the "**Parties**."

WHEREAS, Customer wishes to subscribe to the Services (as defined in **Section 2.1**), and iManage wishes to provide such Services to Customer, each on the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definitions.

"**Action**" means any claim, suit, action or proceeding.

"**Affiliate**" of a Party means any other entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Party.

"**Authorized User**" means each of the individuals authorized by Customer to access and use the Services.

"**Cloud Services**" means the cloud-based software-as-a-service applications, including the application programming interfaces, provided by iManage, and subscribed to under an Order.

"**Customer Data**" means data submitted to, and stored within, the Cloud Services by Customer and its Authorized Users in connection with Customer's use of such Cloud Services (and includes any such data held in iManage's backups).

"**Data Protection Agreement**" or "**DPA**" means the agreement set forth in **Exhibit C**.

"**Documentation**" means any manuals, instructions or other documents or materials that iManage provides or makes available to Customer within embedded help files or on the iManage support website found at https://help.imanage.com or https://help.closingfolders.com/hc/en-us, as applicable, and which describe the functionality, components, features or requirements of the Services, including any aspect of their installation, configuration, integration, operation, use, or support.

"**Fees**" means the fees set out in the applicable Order.

"**Harmful Code**" means any software, hardware or other technology, device or means, including any virus, worm, malware or other malicious computer code, the purpose or effect of which is to (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner (i) the function of any computer, software, firmware, hardware, system or network or (ii) the security, integrity, confidentiality or use of any data, or (b) prevent Customer or any Authorized User from accessing or using the Cloud Services as intended by this Agreement.

Previous versions of this Agreement were published on 1 October 2022, 23 May 2022, 16 September 2021, 16 April 2021, 15 May 2020, 11 October 2018, 28 August 2018, 6 March 2017, and 29 August 2016

"**iManage Personnel**" means individuals involved in the performance of Services as employees or independent contractors of iManage.

"**iManage Software**" means software that allows an Authorized User to use certain features of the Cloud Services and is provided by iManage either for installation on Customer's or an Authorized User's device, or that is otherwise accessed by Authorized Users from or through Customer's or an Authorized User's software, hardware, or other devices.

"**Intellectual Property Rights**" means existing and future registered and unregistered rights granted, applied for or otherwise in existence under or related to any patent, copyright, trademark, trade secret, database protection or other intellectual property Laws, and all similar or equivalent rights or forms of protection, in any part of the world.

"**Law**" means any applicable statute, law, ordinance, regulation, rule, order, constitution, treaty, common law, judgment, decree, or other requirement having the force of law, of any federal, state, provincial, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction, whether in existence as of the effective date of this Agreement or promulgated thereafter, as amended, or superseded.

"**Losses**" means any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees.

"**Order**" means the separate ordering document(s) under which Customer subscribes to the Cloud Services pursuant to this Agreement, whether (a) placed by Customer directly with iManage, or (b) placed by a Partner (on behalf of Customer) with iManage, referencing this Agreement, with respect to Customer's subscription to the Cloud Services.

"**Order Effective Date**" means the effective date specified in the applicable Order.

"**Order Term**" means an Order Initial Term (as defined in **Section 7.2**) together with each applicable Order Renewal Term (as defined in **Section 7.3**).

"**Partner**" means an entity that has entered into an agreement ("**Partner Agreement**") with iManage that, among other things, authorizes the entity to resell the Services.

"**Permitted Use**" means any use of the Services and iManage Software, by an Authorized User, for the benefit of Customer solely in or for Customer's internal business operations.

"**Professional Services**" means certain non-recurring professional, educational, operational, or technical services that Customer, at its option, may request from iManage and that iManage agrees to provide pursuant to an agreed upon statement of work ("**SOW**"). Professional Services do not include services undertaken by a Partner.

"**Professional Services Data**" means all data provided to iManage by or on behalf of Customer (or that Customer authorizes iManage to obtain from the Cloud Services), through an engagement with iManage to obtain Professional Services.

"**Regulator**" means any public body, government agency, or regulator with competent jurisdiction over a Party or one of its Affiliates.

"**Representatives**" means, with respect to a Party, that Party's and its Affiliates' employees, officers, directors, consultants, agents, independent contractors, service providers, subcontractors, and legal advisors.

"**Support Data**" means all data provided to iManage by or on behalf of Customer (or that Customer authorizes iManage to obtain from the Cloud Services), during iManage's provision of Support Services (as defined in **Section 13)**.

2. Services.

2.1 Services. iManage shall, during the applicable Order Term, provide to Customer, exercisable by and through Authorized Users, the following services (the "**Services**"), as applicable: (a) the Cloud Services; (b) the Support Services; (c) the Professional Services as set forth in a SOW; and (d) any incidental services not expressly set out in an Order or SOW if they are reasonably and necessarily required for the proper performance of the Services that are expressly set out in the applicable Order or SOW.

2.2 Services Changes. iManage may make commercially reasonable changes to the Cloud Services, Support Services, and iManage Software from time to time; provided that, such change does not materially degrade the performance of the Cloud Services, Support Services, or iManage Software.

2.3 Non-iManage Applications and Services. Customer's use of any third-party applications, services, or products, which are licensed by their provider to Customer and/or Authorized User(s), for use in connection with the Services ("**Third-Party Products**"), and any exchange or other transfer of any information between Customer and any third-party provider ("**Third-Party Data Transfer**") is solely between Customer and the applicable third-party provider. iManage makes no warranties of any kind and assumes no liability whatsoever for Customer's or Authorized Users' use of such Third-Party Products or acts or omissions in connection with any such Third-Party Data Transfer.

2.4 SLA. **Exhibit A** to this Agreement sets forth the service level agreement applicable to the Cloud Services.

3. Authorization and Customer Restrictions.

3.1 Authorization. iManage hereby authorizes Customer to access and use, during the applicable Order Term, the Cloud Services, the iManage Software, and such Documentation as iManage may supply or make available to Customer solely for the Permitted Use by and through Authorized Users in accordance with the Documentation. This authorization is non-exclusive and, except as may be expressly set forth in **Section 12.9**, non-transferable.

3.2 Acceptable Use, Limitations and Restrictions.

(a) Neither Customer nor its Authorized Users may use the Services or the iManage Software: (i) in a way prohibited by Law; (ii) to violate the rights of others; (iii) to try to gain unauthorized access to or disrupt the Services, the iManage Software, or any other service, device, data, account, or network; (iv) to spam or distribute Harmful Code; or (v) in a way that could harm or otherwise impair the Services, the iManage Software, or anyone else's use of it.

(b) Neither Customer nor its Authorized Users may: (i) resell or redistribute the Services or the iManage Software, (ii) allow multiple users to directly or indirectly access any Services or iManage Software feature that is made available on a per-user basis, (iii) access the Services or the iManage Software in order to build a competitive product or service, (iv) reverse engineer the Cloud Services or the iManage Software (except to the extent permitted by Law without possibility of contractual waiver), or (v) perform significant load or security testing.

(c) Without limiting any of iManage's other rights under this Agreement, an Authorized User's actual or suspected violation of the terms in this **Section 3.2** may result in suspension of such Authorized User's use of the Services or the iManage Software. iManage will suspend such Authorized User's use of the Services and the iManage Software only to the extent, and for the time period, reasonably necessary to address said violation. Unless iManage believes an immediate suspension is required, iManage will provide reasonable notice before suspending the Authorized User's use of the Services or the iManage Software. iManage may seek all reasonable legal remedies available to it if a violation of this **Section 3.2** occurs. For the avoidance of doubt, the suspension rights in this Section only apply to those Authorized Users whom iManage knows or reasonably suspects are in violation of **Section 3.2** (and not to Customer generally).

3.3 Use by Affiliates. Customer is entitled to make the Services, the iManage Software, and Documentation available to Authorized Users of its Affiliates provided that: (a) Customer will be responsible for the Fees and all acts and omissions of its Affiliates (and their Authorized Users); (b) Customer is liable for ensuring that its Affiliates (and their Authorized Users) comply with the terms of this Agreement; and (c) Customer shall ensure that any rights or remedies arising in connection with this Agreement will be actionable against iManage solely by Customer and not by any Affiliate except that Customer will be entitled to treat Losses of its Affiliates as if they are Losses of Customer.

3.4 iManage Software. Customer may need to install certain iManage Software in order to use the Cloud Services. If so, during the applicable Order Term, Customer may install and use the iManage Software only for use with the Cloud Services. Customer must uninstall the iManage Software when Customer's right to use the Cloud Services ends.

4. Fees; Payment Terms. In the event that a Partner places an Order with iManage on Customer's behalf, only **Section 4.8** of this **Section 4** shall apply to Customer.

4.1 Fees. Customer shall pay iManage the Fees in accordance with this **Section 4**. Fees shall be paid in the currency as detailed in the applicable Order.

4.2 Non-refundable and No Cancellation. Except as specifically set forth in this Agreement, all Orders, including all payment obligations thereunder, are non-cancelable and all payments made are non-refundable.

4.3 Taxes. Orders pursuant to this Agreement do not include any transaction taxes, which may include local, state, provincial, federal, or foreign taxes, levies, duties, or similar governmental assessments of any nature, including value-added taxes, excise, use, goods and services taxes, consumption taxes or similar taxes (collectively defined as "**General Taxes**"). All Fees invoiced pursuant to this Agreement are payable in full and without reduction for General Taxes and/or foreign withholding taxes (collectively defined as "**Taxes**"). Customer is responsible for paying all Taxes associated with Fees due pursuant to this Agreement and all Orders, excluding income taxes imposed on iManage ("**iManage Income Tax**"). If iManage has a legal obligation to pay or collect Taxes (expressly excluding iManage Income Tax) for which Customer is responsible under this Agreement, the appropriate amount shall be computed based on Customer's address listed in the applicable Order and invoiced to and paid by Customer. Customer hereby confirms that iManage can rely on the sold-to name and address set forth in the Order(s) that Customer places with iManage as being the place of supply for purposes of any General Tax. If Customer is legally entitled to an exemption from the payment of any Taxes, Customer will promptly provide iManage with legally sufficient tax exemption certificates for each taxing jurisdiction for which it claims exemption.

4.4 Disputed Fees. If Customer disputes any portion of Fees set forth on any invoice, Customer shall within thirty (30) days of the date of the applicable invoice (a) pay the undisputed portion of Fees on said invoice and (b) notify iManage, in writing, of its basis for contesting the disputed Fees. The Parties agree to discuss any dispute within ten (10) days of iManage's receipt of such notification. If necessary, iManage shall provide an amended invoice to Customer after the discussion and Customer will pay such invoice within the time period set forth in the applicable Order.

4.5 Late Payment. If Customer fails to make any undisputed payment when due then, in addition to all other remedies that may be available, if such failure continues for thirty (30) days following written notice of such failure (including notice that the Cloud Services may be suspended), iManage may suspend performance of the Cloud Services until all past due amounts have been paid, without incurring any obligation or liability to Customer by reason of such suspension. At iManage's discretion, past due amounts may accrue a late fee equal to the lesser of 1.5% per month or the maximum amount allowed by applicable Law.

4.6 No Deductions or Setoffs. All amounts payable to iManage under this Agreement shall be paid by Customer to iManage in full without any setoff, deduction or withholding for any reason (other than any deduction or withholding of tax as may be required by applicable Law).

4.7 Purchase Orders. If Customer requires the use of a purchase order or purchase order number, Customer (a) must provide the purchase order number at the time of purchase and (b) agrees that any terms and conditions on any such purchase order are null and void and will not apply to Customer's procurement of the Services or any other subject matter of this Agreement.

4.8 Purchases Through Partners. Customer may authorize a Partner to place an Order with iManage on Customer's behalf. Partners are not agents of iManage and are not authorized to enter into any agreement with Customer on behalf of iManage. iManage Partners are not authorized to make any promises or commitments on iManage's behalf, and iManage shall have no obligation to Customer other than those obligations specifically set forth and agreed to by iManage and Customer in this Agreement. If Customer orders from a Partner, the Partner will set Customer's pricing and payment terms for that Order, and Customer will pay the amounts due to the Partner. Customer consents to iManage and its Affiliates providing the Partner with Administrator Data (as defined below) for purposes of provisioning, administering, and supporting (if applicable) the Services. The Partner may use such data according to the terms of the Partner's agreement with Customer. "**Administrator Data**" means the information provided to iManage or its Affiliates during sign-up, purchase, or administration of the Services. Under the terms and conditions of the applicable Partner Agreement, iManage is entitled to suspend or terminate Customer's subscription to the Cloud Services, Customer's rights to access and use the Cloud Service, and remove and discard any Customer Data (pursuant to the terms herein), if iManage is notified by Partner of Customer's failure to pay amounts due to Partner with respect to Customer's subscription to the Cloud Services; provided that, if Customer properly pays Partner, failure by such Partner to make any requisite payments to iManage shall not affect the validity or enforceability of iManage's obligations hereunder, nor shall it affect the validity of any access and use right which is subject to this Agreement. Customer consents to this suspension and termination right and acknowledges and agrees that iManage shall have no liability to Customer of any kind with respect to any such suspension or termination. Customer's sole recourse with respect to any such suspension or termination shall be against Partner.

5. Intellectual Property Rights.

5.1 Services and Documentation. All right, title, and interest in and to the Services, the iManage Software, and Documentation, including all Intellectual Property Rights therein, are and will remain with iManage. Customer has no right, license, or authorization with respect to any of the Services or Documentation except as expressly set

forth in **Section 3.1**, in each case subject to **Section 3.2**. All other rights in and to the Services, the iManage Software, and Documentation are expressly reserved by iManage.

5.2 Customer Data. As between Customer and iManage, Customer is and will remain the sole and exclusive owner of all right, title, and interest in and to all Customer Data, including all Intellectual Property Rights relating thereto.

6. Confidentiality and Security.

6.1 Confidential Information. In connection with this Agreement, each Party or one of its Affiliates (as the "**Disclosing Party**") may disclose or make available Confidential Information to the other Party or one of its Affiliates (as the "**Receiving Party**") (including Confidential Information that might be disclosed through, or to, a Partner). Subject to **Section 6.2**, "**Confidential Information**" means information in any form or medium (whether oral, written, electronic or other) disclosed, or made available, by a Party, or on behalf of a Party, to the other Party that is identified as confidential at time of disclosure or is disclosed, or made available, under circumstances that would reasonably indicate confidential treatment, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know-how, business operations, plans, strategies, customers, pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations, in each case whether or not marked, designated or otherwise identified as "confidential". Without limiting the foregoing, (a) all Customer Data, Professional Services Data and Support Data is and will remain the Confidential Information of Customer, (b) the Services, iManage Software and Documentation are and will remain the Confidential Information of iManage and (c) the terms and existence of this Agreement are Confidential Information of each Party with respect to the other.

6.2 Exclusions. Confidential Information does not include information that the Receiving Party can demonstrate by written or other documentary records: (a) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information's being disclosed or made available to the Receiving Party in connection with this Agreement; (b) was or becomes generally known by the public other than by the Receiving Party's or any of its Representatives' noncompliance with this Agreement; (c) was or is received by the Receiving Party on a non-confidential basis from a third party that, to the Receiving Party's knowledge, was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; or (d) was or is independently developed by the Receiving Party without reference to or use of any Confidential Information.

6.3 Protection of Confidential Information. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party shall:

(a) not access or use Confidential Information other than as necessary to exercise its rights or perform its obligations under and in accordance with this Agreement;

(b) except as may be permitted by and subject to its compliance with **Section 6.4**, not disclose or permit access to Confidential Information other than to its Representatives who: (i) need to know such Confidential Information for purposes of the Receiving Party's exercise of its rights or performance of its obligations under and in accordance with this Agreement; (ii) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this **Section 6.3**; and (iii) are bound by confidentiality and restricted use obligations at least as protective of the Confidential Information as the terms set forth in this **Section 6.3**;

(c) safeguard the Confidential Information from unauthorized use, access or disclosure using at least the degree of care it uses to protect its sensitive information and in no event less than a reasonable degree of care: (i) with respect to trade secrets, for so long as such trade secrets qualify as trade secrets under applicable Law, (ii) with respect to Customer Data, in perpetuity, and (iii) with respect to all other Confidential Information, for five (5) years from the date of receipt or for such period as the information remains confidential, whichever is longer; and

(d) ensure its Representatives' compliance with and be responsible and liable for any of its Representatives' non-compliance with, the terms of this **Section 6**.

6.4 Compelled Disclosures. If the Receiving Party or any of its Representatives is compelled by applicable Law or a Regulator to disclose any Confidential Information then, to the extent permitted by applicable Law or such Regulator, the Receiving Party shall: (a) promptly, and prior to such disclosure, notify the Disclosing Party in writing of such requirement so that the Disclosing Party can oppose such disclosure, seek a protective order or other limitation on disclosure, or waive its rights under **Section 6.3**; and (b) provide reasonable assistance to the Disclosing Party, at the Disclosing Party's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or the Receiving Party, after providing the notice and assistance required under this **Section 6.4**, remains required by Law or such Regulator to disclose any Confidential Information, the Receiving Party shall disclose only that portion of the

Confidential Information that the Receiving Party is legally required to disclose and, on the Disclosing Party's request, shall use commercially reasonable efforts to obtain assurances from the applicable court or other presiding authority that such Confidential Information will be afforded confidential treatment.

6.5 Additional iManage Obligations Regarding Law Enforcement. iManage will not disclose or provide access to any Confidential Information to law enforcement unless required by Law. If law enforcement contacts iManage with a demand for Confidential Information, iManage will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Confidential Information to law enforcement, iManage will, to the extent permitted by applicable Law or the applicable law enforcement agency, (a) promptly notify Customer and provide a copy of the demand; (b) assess the legitimacy of any request, including the identity of the sender; (c) submit any clarifications necessary to understand the scope of the disclosure request; and (d) oppose any blanket disclosure requests. iManage will not provide any law enforcement agency with: (1) blanket or unfettered access to Confidential Information; (2) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (3) access to Confidential Information if iManage is aware that the data is to be used for purposes other than those stated in the third party's request. In support of the above, iManage may provide Customer's basic contact information to the law enforcement agency.

6.6 Security. During the Agreement Term (as defined in **Section 7.1**), iManage will maintain commercially reasonable technical and organizational measures, including disaster recovery and business continuity procedures, designed to: (a) ensure the security and integrity of Customer Data, and (b) protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. Such security safeguards and measures applicable to Customer Data are further described in **Exhibit B**. Customer is solely responsible for making an independent determination as to whether the technical and organizational measures meet Customer's requirements.

7. Term and Termination.

7.1 Agreement Term. This Agreement shall commence on the first Order Effective Date and, unless terminated earlier pursuant to any of this Agreement's express provisions, will continue for as long as there is an Order in effect (the "**Agreement Term**").

7.2 Order Initial Term. The initial term of an Order commences upon the applicable subscription start date and, unless terminated earlier pursuant to any of this Agreement's express provisions, will continue for the initial term as set forth in the Order (the "**Order Initial Term**").

7.3 Order Renewal Term. Unless otherwise expressly agreed in the applicable Order, each Order will automatically renew for additional successive one-year terms unless earlier terminated pursuant to this Agreement's express provisions or either Party gives the other Party written notice of non-renewal at least thirty (30) days prior to the expiration of the then-current term (each, an "**Order Renewal Term**").

7.4 Termination. In addition to any other express termination right set forth elsewhere in this Agreement, either Party may terminate this Agreement or an Order, effective on written notice to the other Party, if the other Party materially breaches this Agreement or that Order, and such breach: (a) is incapable of cure; or (b) being capable of cure, remains uncured thirty (30) days after the non-breaching Party provides the breaching Party with written notice of such breach with specific reference to the non-breaching Party's right of termination under this **Section 7.4**. Termination of an Order shall not result in the automatic termination of any other Orders in existence.

7.5 Effect of Expiration or Termination. Upon any expiration or termination of this Agreement or an Order, as applicable, except as expressly otherwise provided in this Agreement:

(a) all rights, licenses, consents, and authorizations granted by either Party to the other hereunder will immediately terminate;

(b) Customer shall cease all use of any Services, iManage Software, and Documentation, and (i) promptly return to iManage or, at iManage's written request, destroy all documents and tangible materials containing, reflecting, incorporating, or based on any Documentation or iManage Confidential Information, and (ii) permanently erase all iManage Software, Documentation and iManage Confidential Information from all systems Customer directly or indirectly controls;

(c) notwithstanding anything to the contrary in this Agreement, with respect to information and materials then in its possession or control: (i) the Receiving Party may retain the Disclosing Party's Confidential Information, in its then current state and solely to the extent and for so long as required by applicable Law; (ii) the Receiving Party also may retain the Disclosing Party's Confidential Information in its backups and disaster recovery systems until such Confidential Information is deleted or otherwise remediated in the ordinary course of

business (not to exceed 180 days); and (iii) all information and materials described in this **Section 7.5**(**c**) will remain subject to all confidentiality, security and other applicable requirements of this Agreement;

(d) if Customer properly terminates this Agreement or an Order, Customer will be relieved of any obligation to pay any applicable Fees attributable to the period after the effective date of such termination and iManage will: (i) refund to Customer all Fees paid in advance for Services that iManage has not performed as of the effective date of termination and (ii) pay to Customer any unpaid Service Credit (as defined in **Exhibit A**) to which Customer is entitled (for the avoidance of doubt, the termination of an Order shall not affect the Customer's obligation to pay Fees in respect of any other Orders which continue in existence); and

(e) if iManage properly terminates this Agreement or an Order, all Fees that would have become payable had this Agreement remained in effect until expiration of the applicable Order Term will become immediately due and payable, and Customer shall pay such Fees, together with previously accrued but not yet paid Fees, on receipt of iManage's invoice therefor.

7.6 Surviving Terms. Each provision of this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any termination or expiration of this Agreement.

8. Representations and Warranties.

8.1 Mutual Representations and Warranties. Each Party represents and warrants to the other Party that:

(a) it is duly organized, validly existing and in good standing as a corporation or other entity under the Laws of the jurisdiction of its incorporation or other organization;

(b) it has the full right, power, and authority to enter into and perform its obligations and grant the rights, licenses, consents, and authorizations it grants or is required to grant under this Agreement;

(c) the execution of this Agreement by its representative has been duly authorized by all necessary corporate or organizational action of such Party; and

(d) this Agreement will constitute the legal, valid, and binding obligation of such Party, enforceable against such Party in accordance with its terms.

8.2 Compliance with Laws.

(a) iManage. iManage will comply with all Laws applicable to its obligations hereunder in providing the Services. However, iManage is not responsible for compliance with any Laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. iManage does not determine whether Customer Data includes information subject to any specific Law or regulation.

(b) Customer. Customer must comply with all Laws applicable to its use of the Services. Customer is responsible for maintaining privacy protections and security measures for components that Customer provides or controls, and for using the Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of the Services.

8.3 Additional iManage Representations, Warranties and Covenants. iManage represents, warrants and covenants to Customer, during the Agreement Term, that (a) iManage will perform the Services using personnel of required skill, experience and qualifications and in a professional and workmanlike manner in accordance with generally recognized industry standards for similar services and will devote adequate resources to meet its obligations under this Agreement, (b) the Cloud Services are and will remain free of Harmful Code, and (c) the Cloud Services will perform substantially in accordance with the functions specified in the Documentation when under use by Authorized Users in a manner that conforms to the terms and conditions of this Agreement and the Documentation. The warranties set forth herein are made to and for the benefit of Customer only.

8.4 Additional Customer Representations, Warranties and Covenants. Customer represents, warrants and covenants to iManage, during the Agreement Term, that (a) Customer is responsible for use of the Services by Authorized Users, and for ensuring that Authorized Users comply with the terms of this Agreement, (b) Customer owns or otherwise has and will have the necessary rights and consents in and relating to Customer Data as necessary in order to grant the rights to iManage contemplated by this Agreement, and (c) iManage's Processing (as defined below) of Customer Data in accordance with the terms hereof does not, and will not, cause iManage to suffer any liability for violation of a third party's rights, or violation of any applicable Law.

8.5 DISCLAIMER OF WARRANTIES. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, ALL SERVICES, IMANAGE SOFTWARE, AND DOCUMENTATION ARE PROVIDED "AS IS" AND IMANAGE HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHER, AND IMANAGE SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, IMANAGE MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, IMANAGE SOFTWARE OR DOCUMENTATION, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL OPERATE WITHOUT INTERRUPTION, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM OR OTHER SERVICES EXCEPT IF AND TO THE EXTENT EXPRESSLY SET FORTH IN THE DOCUMENTATION, OR BE ERROR FREE.

9. Indemnification.

9.1 iManage Indemnification. iManage shall indemnify, defend, and hold harmless Customer from and against Losses incurred by Customer arising out of or relating to any Action by a third party (other than an Affiliate of Customer) to the extent that such Losses arise from use of the Services, the iManage Software and Documentation (excluding Customer Data) in compliance with this Agreement that infringes an Intellectual Property Right of such third party. The foregoing obligation does not apply to any Action or Losses arising out of or relating to any:

(a) access to or use of the Services, the iManage Software, or Documentation in combination with any hardware, system, software, network or other materials or service not provided or authorized in the Documentation or otherwise in writing by iManage;

(b) modification of the Services, the iManage Software, or Documentation other than: (i) by or on behalf of iManage; or (ii) with iManage's written approval in accordance with iManage's written specification; or

(c) failure to timely implement any modifications, upgrades, replacements, or enhancements that require Customer action to implement, and are made available to Customer by or on behalf of iManage.

9.2 Customer Indemnification. Customer shall indemnify, defend and hold harmless iManage and its Affiliates, and each of its and their respective officers, directors, employees, agents, successors and assigns (each, an "**iManage Indemnitee**") from and against Losses incurred by such iManage Indemnitee in connection with any Action by a third party (other than an Affiliate of an iManage Indemnitee) that arises out of or relates to: (a) Customer Data infringing the Intellectual Property Right of such third party; or (b) Customer's use of the Services in violation of this Agreement or the Documentation.

9.3 Indemnification Procedure. Each Party shall promptly notify the other Party in writing of any Action for which such Party believes it is entitled to be indemnified pursuant to **Section 9.1** or **Section 9.2**. The Party seeking indemnification (the "**Indemnitee**") shall cooperate with the other Party (the "**Indemnitor**") at the Indemnitor's sole cost and expense. The Indemnitor shall immediately take control of the defense and investigation of such Action and shall employ counsel of its choice to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitee's failure to perform any obligations under this **Section 9.3** will not relieve the Indemnitor of its obligations under this **Section 9** except to the extent that the Indemnitor can demonstrate that it has been prejudiced as a result of such failure. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing.

9.4 Mitigation. At its option and sole cost and expense, iManage is entitled to mitigate the risk or Losses of any actual or threatened infringement of any third party's Intellectual Property Right by:

(a) obtaining the right for Customer to continue to use the Services, the iManage Software, and Documentation materially as contemplated by this Agreement;

(b) modifying or replacing the Services, the iManage Software, and Documentation, in whole or in part, to make the Services, the iManage Software, and Documentation (as so modified or replaced) non-infringing, while providing materially equivalent features and functionality, in which case such modifications or replacements will constitute Services, iManage Software, and Documentation, as applicable, under this Agreement; or

(c) if options (**a**) or (**b**) are not commercially reasonable, by written notice to Customer, terminating this Agreement with respect to all or part of the Services, the iManage Software, and Documentation, requiring Customer immediately to cease any use of the Services, iManage Software, and Documentation or any specified part or feature thereof, adjusting Fees going forward, and issuing Customer a refund equal to the balance of any prepaid amount.

9.5 THIS **SECTION 9** SETS FORTH CUSTOMER'S SOLE REMEDIES AND IMANAGE'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED OR ALLEGED CLAIMS THAT THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF (INCLUDING THE SERVICES, THE IMANAGE SOFTWARE, AND DOCUMENTATION) INFRINGES, MISAPPROPRIATES OR OTHERWISE VIOLATES ANY THIRD-PARTY INTELLECTUAL PROPERTY RIGHT.

10. Limitations of Liability.

10.1 EXCLUSION OF DAMAGES. EXCEPT AS OTHERWISE PROVIDED IN **SECTION 10.3**, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, LOSS OF PROFITS, BUSINESS, BUSINESS OPPORTUNITIES, REPUTATION, TURNOVER OR REVENUE, LOSS OF ANTICIPATED SAVINGS OR WASTED EXPENDITURE (INCLUDING MANAGEMENT TIME), LOSS, OR LIABILITY UNDER OR IN RELATION TO ANY OTHER CONTRACT, OR LOSS OF GOODWILL, IN EACH CASE, HOWEVER CAUSED, UNDER ANY THEORY OF LIABILITY, INCLUDING, WITHOUT LIMITATION, CONTRACT, TORT, WARRANTY, NEGLIGENCE OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES. IN SUCH AN EVENT, THIS LIMITATION WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

10.2 CAP ON MONETARY LIABILITY. EXCEPT AS OTHERWISE PROVIDED IN **SECTION 10.3**, IN NO EVENT WILL THE AGGREGATE LIABILITY OF EITHER PARTY UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER, INCLUDING ANY ORDERS, UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY AND OTHERWISE, EXCEED THE GREATER OF (A) THE VALUE OF ALL AMOUNTS PAID BY CUSTOMER UNDER THIS AGREEMENT DURING THE 12 MONTHS PRECEDING THE ACT OR OMISSION ALLEGED TO GIVE RISE TO SUCH LIABILITY, OR (B) $50,000 USD. THE FOREGOING LIMITATION APPLIES NOTWITHSTANDING THE FAILURE OF ANY AGREED OR OTHER REMEDY OF ITS ESSENTIAL PURPOSE. THE LIMITATIONS OF LIABILITY PROVIDED FOR HEREIN WILL APPLY IN AGGREGATE TO EITHER PARTY AND THEIR RESPECTIVE AFFILIATES AND SHALL NOT BE CUMULATIVE. THE EXCLUSIONS AND LIMITATIONS IN THIS SECTION SHALL NOT LIMIT OR OTHERWISE RELIEVE CUSTOMER OF ITS PAYMENT OBLIGATIONS UNDER THIS AGREEMENT OR AN APPLICABLE ORDER.

10.3 Exceptions. The exclusions and limitations in **Section 10.1** and **Section 10.2** do not apply to: (a) fraud or fraudulent misrepresentation of either Party, (b) the liability of either Party for the indemnities set out in **Section 9** (Indemnification), (c) negligence of either Party causing death or personal injury, or (d) liability for willful misconduct.

11. Force Majeure.

11.1 No Breach or Default. In no event will either Party be liable or responsible to the other Party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing this Agreement, except for any payment obligation, when and to the extent such failure or delay is caused by any circumstances beyond such Party's reasonable control (a "**Force Majeure Event**"), including acts of God, flood, fire, earthquake, explosion, other catastrophes, such as epidemics, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Agreement, national or regional emergency, strikes, labor stoppages or slowdowns or other industrial disturbances (other than within iManage), passage of Law or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition or any complete or partial government shutdown, or national or regional shortage of adequate power or telecommunications or transportation. Either Party may terminate this Agreement if a Force Majeure Event continues substantially uninterrupted for a period of thirty (30) days or more.

11.2 Affected Party Obligations. In the event of any failure or delay caused by a Force Majeure Event, the affected Party shall give prompt written notice to the other Party stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

12. Miscellaneous.

12.1 Export Compliance. The Services and other technology iManage makes available, and derivatives thereof, may be subject to export Laws and regulations of the United States and other jurisdictions. Each Party represents that it is not named on any U.S. government denied-party list. Customer shall not permit Authorized Users to access or use any Service in a U.S. embargoed country or in violation of any U.S. export law or regulation.

12.2 Further Assurances. Upon a Party's reasonable request, the other Party shall, at the requesting Party's sole cost and expense, execute and deliver all such documents and instruments, and take all such further actions, necessary to give full effect to this Agreement.

12.3 Contractual Relationship. The Parties are entering into this Agreement as independent contracting parties. Neither Party will have, or hold itself out as having, any right or authority to incur any obligation on behalf of the other Party. This Agreement will not be construed to create an association, joint venture, or partnership between the Parties or to impose any partnership liability upon either Party.

12.4 Marketing. Customer agrees that iManage may include Customer's name and logo on iManage's website and in iManage's list of customers, press releases and other promotional materials.

12.5 Notices. Any notice or other communication under this Agreement given by a Party to the other Party will be in writing and will be effective upon delivery as follows: (i) if to Customer, (1) when delivered via registered mail, return receipt requested, to the address specified in an Order; or (2) when sent via email to the email address specified in an Order or otherwise on record for Customer; and (ii) if to iManage, when sent via email to legal@imanage.com, with a duplicate copy sent via registered mail, return receipt requested, to: Attn: Legal Department, iManage LLC, 71 South Wacker Drive, Suite 400, Chicago, IL, 60606, (or such subsequent address found on https://imanage.com/contact-us/). Any such notice, in either case, must specifically reference that it is a notice given under this Agreement. iManage may provide Customer with information and notices about the Cloud Services electronically, including via email, through the portal for the Cloud Services, or through a web site that iManage identifies, which has a mechanism allowing Customer to subscribe to receive such notifications via email. Notice is given as of the date it is made available by iManage. It is Customer's sole responsibility to ensure that Customer's administrators maintain accurate contact information on the iManage support website found at https://help.imanage.com.

12.6 Interpretation. For purposes of this Agreement: (a) the words "include," "includes" and "including" are deemed to be followed by the words "without limitation"; (b) the word "or" is not exclusive; (c) the words "herein," "hereof," "hereby," "hereto" and "hereunder" refer to this Agreement as a whole; (d) words denoting the singular have a comparable meaning when used in the plural, and vice-versa; and (e) words denoting any gender include all genders. Unless the context otherwise requires, references in this Agreement: (x) to sections, exhibits, schedules, attachments and appendices mean the sections of, and exhibits, schedules, attachments and appendices attached to, this Agreement; (y) to an agreement, instrument or other document means such agreement, instrument or other document as amended, supplemented and modified from time to time to the extent permitted by the provisions thereof; and (z) to a statute means such statute as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder. The Parties intend this Agreement to be construed without regard to any presumption or rule requiring construction or interpretation against the Party drafting an instrument or causing any instrument to be drafted. The exhibits, schedules, and appendices referred to herein are an integral part of this Agreement to the same extent as if they were set forth herein.

12.7 Headings. The headings herein are for reference only and do not affect the interpretation of this Agreement.

12.8 Entire Agreement. This Agreement, together with any other documents incorporated herein by reference, constitutes the sole and entire agreement of the Parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related exhibits, schedules, attachments, and appendices (other than an exception expressly set forth as such therein) and any other documents incorporated herein by reference, the following order of precedence governs: (a) first, the exhibits to this Agreement; (b) second, the main body of this Agreement; and (c) third, any other documents incorporated herein by reference.

12.9 Assignment. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other Party's prior written consent (not to be unreasonably withheld); provided, however, either Party may assign this Agreement in its entirety (together with all Orders), without the other Party's consent to an Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. Notwithstanding the foregoing, if a Party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favor of, a direct competitor of the other Party, then such other Party may terminate this Agreement upon written notice. In the event of such a termination, iManage will refund to Customer the balance of any prepaid amount. Any purported assignment, delegation, or transfer in violation of this **Section 12.9** is void. This Agreement is binding upon and inures to the benefit of the Parties and their respective permitted successors and permitted assigns.

12.10 No Third-party Beneficiaries. Subject to **Section 9**, this Agreement is for the sole benefit of the Parties and their respective permitted successors and permitted assigns and nothing herein, express, or implied, is intended to or shall confer upon any other entity or natural person any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

12.11 Modification, Amendment and Waiver. Except as otherwise provided herein, no modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by the Party against whom the modification, amendment or waiver is to be asserted.

12.12 Severability. If any provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate

or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties shall negotiate in good faith to modify this Agreement so as to affect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby may be consummated as originally contemplated to the greatest extent possible.

12.13 iManage Entity, Applicable Law, and Venue.

(a) The iManage entity entering into this Agreement depends on the billing address of Customer set forth in the applicable Order. If the billing address is located in Europe, the Middle East or Africa, the iManage entity entering into this Agreement is iManage EMEA Limited, a private limited company registered in England and Wales. If the billing address is located in any other region, the iManage entity entering into this Agreement is iManage LLC, a Delaware limited liability company.

(b) This Agreement shall be governed by and construed in accordance with the Laws as set forth in the table below, without giving effect to conflict of law or choice of law principles. Any and all actions, suits or judicial proceedings upon any claim arising from or relating to this Agreement shall be instituted and maintained in the city, state, territory, or province, as applicable, set forth in the table below. If either Party may file an action, suit or judicial proceeding in a federal court, such action, suit, or judicial proceeding shall be in a federal court seated in the state, territory, or province, as applicable, as set forth in the table below. This choice of jurisdiction does not prevent either Party from seeking injunctive relief with respect to a violation of Intellectual Property Rights.

If Customer is domiciled in:	**The governing Law is:**	**Venue lies exclusively in courts sitting in:**
The United States of America, Mexico, or a country in Central or South America or the Caribbean	Illinois and controlling United States federal law	Chicago, Illinois, USA
A country in Europe, the Middle East, or Africa	England	London, England
United Kingdom	England	London, England
Canada	Ontario and controlling Canadian federal law	Toronto, Ontario, Canada
Japan	Japan	Tokyo, Japan
A country in Asia or the Pacific region, other than Japan, Australia, or New Zealand	Singapore (as described in **Section 12.13(c)**)	Singapore (as described in **Section 12.13(c)**)
Australia or New Zealand	New South Wales, Australia and controlling Australian federal law	New South Wales, Australia

(c) If Customer's principal place of business is in a country in Asia or the Pacific region, other than Japan, Australia or New Zealand, any dispute arising out of or in connection with this Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration in Singapore in accordance with the Arbitration Rules of the Singapore International Arbitration Centre, which rules are deemed to be incorporated by reference into this subsection. The Tribunal shall consist of one arbitrator. The language of the arbitration shall be English. The decision of the arbitrator shall be final, binding, and incontestable and may be used as a basis for judgment thereon in the above-named countries or elsewhere. To the maximum extent permitted by applicable Law, the Parties waive their right to any form of appeal or other similar recourse to a court of law.

12.14 Waiver of Jury Trial. Each Party irrevocably and unconditionally waives any right it may have to a trial by jury in respect of any legal action arising out of or relating to this Agreement or the transactions contemplated hereby.

12.15 Equitable Relief. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under **Section 6** or, in the case of Customer only, **Section 3.1** or **Section 3.2**, may cause the

other Party irreparable harm for which monetary damages may not be an adequate remedy and agrees that, in the event of such breach or threatened breach, the other Party will be entitled to seek equitable relief, including a restraining order, an injunction, specific performance and any other relief that may be available from any court, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at Law, in equity or otherwise.

12.16 Anti-Corruption. Each Party agrees that it has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of the other Party's employees, agents, or subcontractors in connection with this Agreement. Each Party will use reasonable efforts promptly to notify the other Party should such Party learn of any violation of this restriction.

12.17 Government Users. If Customer is a U.S. government entity or if this Agreement otherwise becomes subject to the Federal Acquisition Regulations (FAR), Customer acknowledges that elements of the Cloud Services constitute software and documentation and are provided as "Commercial Items" as defined at 48 C.F.R. § 2.101 and are being licensed to U.S. government user as commercial computer software subject to the restricted rights described in 48 C.F.R. §§ 2.101 and 12.212.

12.18 Feedback. iManage welcomes suggestions, comments, and other feedback on the Services ("**Feedback**") from all of its customers, as it helps iManage to improve its products and services. If Customer provides iManage with Feedback, Customer agrees that: (a) iManage is not subject to any confidentiality obligations in respect to the Feedback; (b) the Feedback is not confidential or proprietary information belonging to Customer or any third party and Customer has all of the necessary rights to disclose the Feedback to iManage; (c) iManage may freely use Feedback without any restrictions; and (d) Customer is not entitled to receive any compensation or reimbursement of any kind for Feedback.

13. Support Services.

13.1 Support Services. The Services include the Support Services as defined as Cloud Services Care and described in the Support Services Terms then in effect, available at:

https://support.imanage.com/worksite/iManage_Maintenance_Terms.pdf (the "**Support Services Terms**").

iManage may amend the Support Services Terms from time to time in its sole discretion; provided that, no such modification will materially degrade the level of service or other benefits provided to Customer under the version of the Support Services Terms in place as of the date of this Agreement, unless such modification has been agreed upon in writing by Customer. In the event the Support Services Terms contain an equivalent term as that in this Agreement, or there is a conflict between a term in the Support Services Terms and this Agreement, the terms in this Agreement shall prevail.

If the Cloud Services are subscribed to through a Partner that is authorized to provide Support Services, the Partner will provide details on the Support Services. In such a situation, the Support Services may be performed by the Partner or its designee, which, in some cases, may be iManage.

Notwithstanding the foregoing, with regard to the Cloud Service known as Closing Folders, iManage will provide Customer with general technical support services to help Customer troubleshoot any technical questions or issues Customer encounters with Closing Folders. iManage will also provide Customer with access to the knowledge base and other technical resources at https://help.closingfolders.com/hc/en-us or such other website as notified to Customer from time to time.

13.2 Support Data; Ownership. Support Data will be used only to provide Support Services. iManage will not use Support Data or derive information from it for any advertising or similar commercial purposes. iManage will delete or return all copies of Support Data after the business purposes for which the Support Data was collected or transferred have been fulfilled or earlier upon Customer's request unless applicable Law requires storage of the Support Data. As between the Parties, Customer retains all right, title, and interest in and to Support Data. iManage acquires no rights in Support Data, other than the rights Customer grants to iManage to provide the Support Services. Customer agrees not to provide any Support Data to iManage to which regulations under FERPA (as defined below) or HIPAA (as defined below) would apply.

14. Professional Services.

14.1 Professional Services. iManage shall provide the Professional Services to Customer as described in an accompanying SOW. In the event of any inconsistencies between this Agreement and a SOW issued under this Agreement, the terms of this Agreement shall take precedence (other than an exception expressly set forth as such in the SOW). To the extent payment terms are not specified in the SOW, the payment terms in this Agreement shall apply.

14.2 License for Deliverables. Upon Customer's payment of fees due under an applicable SOW, iManage grants Customer a worldwide, perpetual, non-exclusive, non-transferable, royalty-free license to copy, maintain, use and run (as applicable), solely for Customer's internal business purposes associated with Customer's use of the Cloud Services and the iManage Software, all documents, work product and other materials (excluding without limitation computer code, algorithms and machine learning models) that are prepared by iManage for Customer pursuant to an applicable SOW ("**Deliverables**"). iManage retains all ownership rights in the Deliverables.

14.3 Representation and Warranty. iManage shall perform the Professional Services pursuant to **Section 8.3**. Customer acknowledges that iManage's ability to successfully perform the Professional Services is dependent upon Customer's provision of timely information, access to resources, and participation. If through no fault or delay of Customer, the Professional Services do not conform to the foregoing warranty, and Customer notifies iManage within sixty (60) days of iManage's delivery of the Professional Services, iManage will either re-perform the non-conforming portions of the Professional Services at no cost to Customer or waive or return, as applicable, any Fees owed or paid for the non-conforming portions of the Professional Services as Customer's sole remedy for breach of this Professional Services warranty.

14.4 THE REMEDIES SET FORTH IN **SECTION 14.3** SHALL BE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND IMANAGE'S ENTIRE LIABILITY FOR ANY BREACH OF THE LIMITED WARRANTY SET FORTH IN **SECTION 14.3**.

14.5 Professional Services Data; Ownership. Professional Services Data will be used only to provide Professional Services. iManage will not use Professional Services Data or derive information from it for any advertising or similar commercial purposes. iManage will delete or return all copies of Professional Services Data after the business purposes for which the Professional Services Data was collected or transferred have been fulfilled or earlier upon Customer's request unless applicable Law requires storage of the Professional Services Data. As between the Parties, Customer retains all right, title, and interest in and to Professional Services Data. iManage acquires no rights in Professional Services Data, other than the rights Customer grants to iManage to provide the Professional Services to Customer. Customer agrees not to provide any Professional Services Data to iManage to which regulations under FERPA or HIPAA would apply.

Exhibit A

Service Level Agreement

1) Service Levels. iManage will make the Cloud Services available for access and use by Customer and its Authorized Users in each Region (as defined below) ("**Available**" and "**Unavailable**" will be interpreted accordingly) at least 99.9% of the time as measured over the course of each calendar month during the applicable Order Term, excluding unavailability of the Cloud Services due to Scheduled Downtime (as defined in **paragraph (6)** below) or any of the Exceptions (as defined below).

"**Exceptions**" mean performance or availability issues: (a) due to a Force Majeure Event; (b) that result from the use of services, hardware, or software not provided by iManage, including issues resulting from inadequate bandwidth or related to third-party software or services; (c) caused by software that is not being run by iManage itself as part of the Cloud Services; (d) during or with respect to beta or trial versions of the Cloud Services, features or software; (e) that result from Customer's unauthorized action or lack of action when required, or from Customer's employees, agents, contractors, or vendors, or anyone gaining access to iManage's network by means of Customer passwords or equipment, or otherwise resulting from Customer's failure to follow appropriate security practices; or (f) that result from Customer's failure to adhere to any required configurations, use supported platforms, or follow any policies for acceptable use, or from Customer's use of the Cloud Services in a manner inconsistent with the features and functionality of the Cloud Services (for example, attempts to perform operations that are not supported) or inconsistent with the Documentation.

"**Region**" means the applicable region(s) accommodating the data center(s) from which the Cloud Services are provisioned, as detailed in the relevant Order.

Availability of the Cloud Services shall be calculated on a per Region basis, as follows:

$$\left[\left(\frac{total - nonexcluded - excluded}{total - excluded}\right) \times 100\right]$$

Where:

- ***total*** means the total number of minutes in the calendar month in the applicable Region;
- ***nonexcluded*** means the total number of minutes in the calendar month where the Cloud Services is Unavailable in the applicable Region, excluding Unavailability of the Cloud Services due to Scheduled Downtime or any of the Exceptions; and
- ***excluded*** means the total number of minutes in the calendar month where the Cloud Services is Unavailable in the applicable Region due to Scheduled Downtime or any of the Exceptions.

The service levels and Service Credits set forth in this **Exhibit A** do not apply to on-premises software licensed as part of Customer's subscription.

2) Claims.

a) In order for iManage to consider a claim for Service Credit, Customer must submit the claim to iManage customer support including all information necessary for iManage to validate the claim, including: (i) the affected Region; (ii) a detailed description of the incident; (iii) information regarding the time and duration of the downtime; (iv) the number and location(s) of affected Authorized Users (if applicable); and (v) descriptions of attempts to resolve the incident at the time of occurrence.

b) iManage must receive the claim by the end of the calendar month following the month in which the incident occurred. For example, if the incident occurred on February 15th, iManage must receive the claim and all required information by March 31st.

c) iManage will evaluate all information reasonably available to iManage and make a good faith determination of whether a Service Credit is owed. iManage will use commercially reasonable efforts to process claims during the subsequent month and within thirty (30) days of receipt. Customer must be in compliance with this Agreement in order to be eligible for a Service Credit.

3) Service Credits.

a) If iManage determines that a Service Credit is owed to Customer pursuant to **paragraph (2)** above, iManage shall apply the Service Credit to Customer as set forth in the table below (each, a "**Service Credit**"). Service Credits are awarded on a per Region basis. Where fees for the Cloud Services are not allocated on a per Region basis in the relevant Order, the Service Credit shall be calculated by dividing the total monthly fee (or 1/12th of the total annual subscription fee, as applicable) by the number of Regions. For the avoidance of doubt,

Unavailability of the Cloud Services in one Region will not result in Service Credits being awarded in respect of any other Region where the Cloud Services are Available.

Service Level	Service Credit (% of 1/12th of the annual subscription fee, for the affected Region)
Less than 99.9% but not less than 99.0%	10%
Less than 99.0% but not less than 98.0%	25%
Less than 98.0% but not less than 95.0%	50%
Less than 95.0%	100%

b) Subject to **paragraph (4)** below, Service Credits are Customer's sole and exclusive remedy for any availability issues under this Agreement. Customer may not unilaterally offset for any performance or availability issues.

c) Service Credits apply only to Fees paid for the particular Cloud Service for which the service level has not been met. The Service Credits awarded with respect to any billing month, for the affected Region, will not, under any circumstance, exceed the Fees for the particular Cloud Service in such billing month for that Region.

4) Termination. Customer may terminate this Agreement, effective on written notice to iManage, in the event the Cloud Services are Available less than 99.0% in any three months, in the same Region, during any consecutive six (6) month period. In such an event, iManage will issue Customer a refund equal to the balance of any prepaid amount.

5) Service Monitoring, Management and Reporting. iManage shall continuously monitor and manage the Cloud Services. Customer may subscribe to Cloud Services notifications and, during the applicable Order Term, iManage will provide such notifications when an issue begins, while the issue is ongoing and when the issue has been resolved. Additionally, iManage publishes Availability reports on the iManage Data Center Alerts page of the iManage support website found at https://help.imanage.com and Customer may subscribe to receive a notification when such reports are published.

6) Scheduled Downtime. iManage reserves the right to schedule downtime for routine maintenance of the Cloud Services in each Region ("**Scheduled Downtime**"). iManage shall use commercially reasonable efforts to provide prior notice to Customer at least seven (7) calendar days before any Scheduled Downtime.

7) Emergency Maintenance. iManage reserves the right to perform emergency maintenance services at any time and without prior notice to Customer; provided that, iManage will use commercially reasonable efforts to provide prior notice to Customer. For the sake of clarity, emergency maintenance shall not be considered an Exception.

8) Pre-Production, Development, Testing and Similar Environments. The service levels and Service Credits set forth in this **Exhibit A** do not apply to Customer's pre-production, development, testing, or similar environments.

9) Previews, Proof-of-Concepts and Trials. Previews, proof-of-concepts, and trials ARE PROVIDED "AS-IS," "WITH ALL FAULTS," AND "AS AVAILABLE," as described herein. The service levels and Service Credits set forth in this **Exhibit A** do not apply to previews, proof-of-concepts, or trials. iManage may change or discontinue previews at any time without notice. iManage may also choose not to make a preview generally commercially available.

Exhibit B

General Security Exhibit

1) Purpose. This **Exhibit B** summarizes the technical and organizational measures that iManage has implemented to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, which are iManage's only responsibility with respect to the security of Customer Data. iManage may adapt such measures from time to time, for example, as a result of the development of regulations, technology, and other industry considerations.

2) Information Security Management. iManage has appointed one or more security officers responsible for coordinating and monitoring security rules and procedures. iManage maintains an information security program designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The information security program may be updated from time to time based on changes in applicable legal and regulatory requirements, best practices and industry standards related to privacy and data security.

3) Standards. iManage uses commercially reasonable and appropriate methods and safeguards to protect the confidentiality, availability, and integrity of Customer Data. iManage adheres, and at all times will adhere, to information security practices at least as protective of Customer Data as identified in ISO 27001 and ISO 27017 (or substantially equivalent or replacement standards) or other generally accepted authoritative standards (*e.g.*, SSAE 16, SOC2).

4) iManage Personnel. iManage maintains written policies and procedures that address the roles and responsibilities of iManage Personnel, including both technical and non-technical personnel, who have access to Customer Data in connection with providing the Cloud Services. All iManage Personnel with access to Customer Data receive annual training. iManage ensures that access rights are revoked for all iManage Personnel immediately upon the termination of their employment, contractual or other relationships with iManage.

5) Information Security Infrastructure.

   a) Asset Inventory. iManage maintains inventories of all media on which Customer Data is stored. Access to such inventories is restricted to authorized iManage Personnel.

   b) Access Controls for iManage Personnel.

      i) Access Policy. iManage enforces an access control policy (physical, technical, and administrative) based on least privileges principles.

      ii) Access Authorization.

         (1) iManage maintains an authorization management system designed to ensure that only authorized iManage Personnel (technical and non-technical) are granted access to systems containing Customer Data.

         (2) All iManage Personnel accessing systems containing Customer Data have a separate, unique username. Deactivated and expired usernames are not recycled or otherwise granted to other individuals.

         (3) iManage restricts access to Customer Data solely to iManage Personnel who have a need to access Customer Data in connection with the Cloud Services or as otherwise required by applicable Law.

      iii) Authentication.

         (1) iManage uses industry standard practices, including strong authentication, to identify and authenticate all iManage Personnel who attempt to access iManage network or information systems.

         (2) Where authentication credentials of iManage Personnel are based on passwords, iManage requires that such passwords meet minimum requirements for length and complexity. iManage maintains practices designed to ensure the confidentiality and integrity of passwords when assigned, distributed, and stored.

         (3) Accounts of iManage Personnel are locked out in case of repeated attempts to gain access to the information system using an invalid password.

   c) Encryption. iManage encrypts Customer Data at rest within the Cloud Services using ciphers at least as strong as 256-bit AES. Customer Data in transit to and from the Cloud Services is transferred to/from the Cloud Services across encrypted network connections and/or protocols (*i.e.*, HTTPS and/or VPN). Backups of Customer Data are encrypted and stored in a secondary data center.

   d) Encryption with Customer Key. Customer assumes all risks of data deletion, inaccessibility, and service outages that result from any unavailability of an encryption key created or maintained solely by Customer (such as the private key in a public-private pair), or where unavailability of any encryption key is caused by an act or omission of Customer or any Authorized User.

e) Network and Host Security.

i) Network Security. iManage utilizes an enterprise-class security information and event management (SIEM) system and maintains firewalls and other control measures (*e.g.*, security appliances, network segmentation) to provide reasonable assurance that access from and to its networks is appropriately controlled.

ii) Security Updates. iManage uses commercially reasonable efforts to ensure that the Cloud Services operating systems and applications that are associated with Customer Data are patched and otherwise secured to mitigate the likelihood and impact of security vulnerabilities in accordance with iManage's patch management processes and within a reasonable time after iManage has actual or constructive knowledge of any critical or high-risk security vulnerabilities. iManage conducts vulnerability testing on a monthly basis.

iii) Malicious Software. iManage maintains anti-malware controls to help prevent malicious software from causing accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

f) Physical Security.

i) iManage maintains physical security safeguards at any facilities where iManage hosts Customer Data. Physical access to such facilities is only granted following a formal authorization procedure and access rights are reviewed periodically.

ii) Such facilities are rated as Tier 3 data centers or greater, and access to such facilities must be limited to identified and authorized individuals. Such facilities use a variety of industry standard systems to protect against loss of data due to power supply failure, fire, and other natural hazards.

g) Backups. iManage provides 24/7 managed backup services that include Customer Data stored in the primary site backed up on at least a daily basis to a secondary site. iManage provides backup services for all components of the solution included in the Cloud Services. Backups are maintained for a period of ninety (90) days in the primary data center, and ninety (90) days in the secondary data center. Notwithstanding the foregoing, the Cloud Service known as Closing Folders only maintains backups for thirty (30) days.

h) Data Management. iManage maintains commercially reasonable controls for information governance and data management in connection with the Cloud Services. iManage destroys, deletes, or otherwise makes irrecoverable Customer Data upon the disposal or removal of storage media. Customer Data for each Customer is logically separated from data of other iManage customers.

6) Independent Assessments. On an annual basis, iManage has an independent third-party organization conduct an independent assessment of the standards set forth in **paragraph (3)** of this **Exhibit B**. Additionally, iManage undergoes penetration testing, conducted by an independent third-party organization, on an annual basis. Upon Customer's request (not more than one time per calendar year), and subject to the confidentiality and non-disclosure obligations set forth in this Agreement, iManage shall make available to Customer information regarding iManage's compliance with the obligations set forth in this Agreement in the form of iManage's ISO 27001 certification and/or SOC 2 or SOC 3 reports.

7) Business Continuity and Disaster Recovery. iManage maintains a business continuity plan that is compliant with ISO 22301. iManage also maintains disaster recovery capabilities designed to minimize disruption to the Cloud Services. Included within these plans is disaster recovery incident management, procedures for the recovery of access to Customer Data in the secondary data center, as well as the periodic testing/exercising of the disaster recovery plan.

8) Customer's Responsibility. Notwithstanding anything contained in this **Exhibit B**, Customer understands and acknowledges that Customer is solely responsible for implementing and maintaining appropriate security measures for all systems within Customer's control. Failure to maintain appropriate security measures by Customer may relieve iManage for any Security Incident (as defined in **Exhibit C**), if such Security Incident was a result of Customer's failure.

Exhibit C

Data Protection Agreement

The Parties agree that this DPA sets forth their obligations with respect to the Processing of Customer Data and Personal Data.

1. Definitions.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations and any amendments thereto.

"**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Law, the Controller or the specific criteria for its nomination may be provided for by such Law.

"**Data Importer**" and "**Data Exporter**" have the meanings set forth in the Standard Contractual Clauses, in each case irrespective of whether such Standard Contractual Clauses, European Data Protection Legislation or Non-European Data Protection Legislation applies.

"**Data Protection Legislation**" means, as applicable, (a) European Data Protection Legislation, and (b) Non-European Data Protection Legislation, which applies to the Processing of Personal Data.

"**Data Subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"**European Data Protection Legislation**" means, as applicable, data protection and privacy legislation in force inside the European Economic Area, including the General Data Protection Regulation and any national Laws implementing such legislation.

"**General Data Protection Regulation**" or "**GDPR**" means Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data.

"**Non-European Data Protection Legislation**" means data protection or privacy legislation in force outside the European Economic Area, including without limitation such legislation as is in force in the United States (including the CCPA and other federal and state Laws, as applicable), UK (including the UK GDPR and national implementing legislation), Brazil, Canada, Australia, Switzerland, and Singapore.

"**Personal Data**" means any information Processed by iManage that relates to a Data Subject and is obtained as either Customer Data, Professional Services Data, or Support Data.

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

"**Processor**" means a natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of a Controller.

"**Pseudonymization**" means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

"**Standard Contractual Clauses**" means as applicable (a) the standard contractual clauses available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR ("**EU SCCs**"); and (b) the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office under S119A(1) of the Data Protection Act available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf ("**UK Addendum**").

"**Sub-Processor**" means other Processors used by iManage to Process Customer Data and Personal Data.

"**Supervisory Authority**" means an independent public authority that has been established by a governmental body and is responsible for monitoring the application of applicable Data Protection Legislation, in order to protect the fundamental rights and freedoms of natural persons in relation to Processing and to facilitate the free flow of Personal Data.

"**UK GDPR**" means the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2. Roles and Scope.

2.1 This DPA only applies to the Processing of Customer Data and Personal Data by iManage on behalf of Customer pursuant to the Agreement.

2.2 Customer and iManage agree that with respect to Personal Data, Customer is the Controller of such Personal Data and iManage is a Processor of such Personal Data, except when Customer acts as a Processor or Sub-Processor of such Personal Data, in which case iManage is a Sub-Processor of such Personal Data. Nothing in the preceding sentence alters the obligations of either iManage or Customer under this DPA, as iManage acts as a Processor with respect to Customer in all events. In any instance where the Customer is a Processor or Sub-Processor, Customer warrants to iManage that Customer's instructions, including appointment of iManage as a Processor or sub-Processor, have been authorized by the relevant Controller.

2.3 This DPA does not limit or reduce any data protection commitments iManage makes to Customer in the Agreement.

2.4 Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Customer Data and Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by iManage provide a level of security appropriate to the risk with respect to its Customer Data and Personal Data.

3. Details of the Processing.

3.1 Data Subjects. The categories of Data Subjects whose Personal Data may be Processed in connection with the Services are determined and controlled by Customer in its sole discretion and may include but are not limited to: Customer's representatives and end users, such as employees, contractors, collaborators, clients, prospects, and customers; and employees or contractors of Customer's clients, prospects, and customers.

3.2 Categories of Personal Data. The categories of Personal Data to be Processed in connection with the Services are determined by Customer in its sole discretion and may include but are not limited to: first and last name, employer, role, professional title, and contact information (*e.g.*, email, phone numbers, and physical address).

3.3 Special Categories of Personal Data. Special categories of Personal Data, if any, to be Processed in connection with the Services are determined by Customer in its sole discretion and may include, but are not limited to, information revealing racial or ethnic origin; political, religious, or philosophical beliefs; trade union membership; or health data.

3.4 Processing Operations. iManage will Process Customer Data and Personal Data only as described and subject to the limitations herein (a) to provide Customer the Services in accordance with the Documented Instructions (as defined below), and (b) for business operations incidental to providing the Services to Customer, which may include (i) delivering functional capabilities as licensed, configured, and used by Customer and its Authorized Users, (ii) preventing, detecting, and repairing problems, including Security Incidents (as defined below), and (iii) providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.

4. Obligations of iManage.

4.1 Processing by iManage shall be governed by the Agreement and this DPA. In particular, iManage shall:

(a) Process Customer Data and Personal Data only on Documented Instructions (as defined below) from Customer, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by applicable Data Protection Legislation; in such a case, iManage shall notify Customer of said legal requirement before Processing, unless said Data Protection Legislation prohibits such notification on important grounds of public interest;

(b) inform Customer if, in its opinion, an instruction given by Customer with regard to Processing of Personal Data infringes any applicable Data Protection Legislation; in such a case, iManage may suspend the relevant Processing without penalty or liability until Customer gives iManage relevant written instructions that in iManage's opinion do not infringe Data Protection Legislation;

(c) ensure that persons authorized to Process Customer Data or Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(d) provide periodic and mandatory data privacy and security training and awareness to iManage Personnel with access to Customer Data or Personal Data in accordance with applicable Data Protection Legislation;

(e) 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, implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, including, those detailed in **Exhibit B** to the Agreement related to Customer Data and, *inter alia*, as appropriate:

(1) the Pseudonymization and encryption of Personal Data;
(2) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services;
(3) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
(4) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

(f) in assessing the appropriate level of security for purposes of **subparagraph 4.1(e)(4)**, take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data transmitted, stored or otherwise Processed;

(g) take steps to ensure that any natural person acting under the authority of iManage who has access to Customer Data or Personal Data does not Process such Personal Data except on instructions from Customer, unless he or she is required to do so by applicable Data Protection Legislation; and

(h) adhere to the conditions set forth in **paragraph 6** below for engaging or changing a Sub-Processor.

4.2 The Parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools made available by iManage for the Cloud Services) constitute Customer's documented instructions regarding iManage's Processing of Customer Data and Personal Data ("**Documented Instructions**"). iManage will Process Customer Data and Personal Data only in accordance with Documented Instructions, and for business operations incidental to providing the Services. Customer hereby grants all such rights and permissions in or relating to Customer Data and Personal Data to iManage and its Sub-Processors, as are necessary to perform the Services. iManage will not retain, use, disclose or otherwise Process Customer Data or Personal Data other than for the purposes set out in this DPA and the Agreement. iManage will not derive information from Customer Data or Personal Data for any advertising or similar commercial purposes. In no event will iManage sell Personal Data.

4.3 Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between iManage and Customer, including agreement on any additional fees payable by Customer to iManage for carrying out such instructions.

5. Security Incident Management.

(a) Notice. iManage will notify Customer of any breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while Processed by iManage (a "**Security Incident**") without undue delay after becoming aware of the Security Incident and, in any event, within 48 hours of becoming aware of such Security Incident. Notification of a Security Incident will be delivered to one or more of Customer's administrators by any means iManage selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain

accurate contact information on the iManage support website found at https://help.imanage.com. Customer is solely responsible for complying with its obligations under incident notification Laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident. iManage's obligation to report or respond to a Security Incident is not an acknowledgement by iManage of any fault or liability with respect to the Security Incident. Similarly, Customer's failure to comply with notification provisions hereunder or otherwise and any liabilities arising therefrom will not be attributed to iManage.

(b) In the event of a Security Incident, iManage will (i) investigate the Security Incident; (ii) provide Customer with information about the Security Incident (including, where possible, the nature of the Security Incident, the contact from whom more information can be obtained, and the likely consequences of the Security Incident), which information may be provided in phases as it becomes available; and (iii) take reasonable steps to mitigate the effects of, and to help minimize any damage resulting from, the Security Incident. In the event that a Security Incident was not due to the fault of iManage, iManage will cooperate with Customer with reasonable costs and expenses to be covered by Customer.

(c) iManage shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable Data Protection Legislation to notify the relevant Supervisory Authority and Data Subjects about such Security Incident.

(d) Customer must notify iManage promptly about any possible misuse of its accounts or authentication credentials or any potential security incident related to a Cloud Service.

6. Sub-Processors.

6.1 iManage may engage subcontractors and Sub-Processors to provide services on its behalf.

6.2 In addition to iManage's Affiliates, Customer consents to iManage engaging the Sub-Processors listed at https://support.imanage.com/resources/Subprocessors.htm for the Processing of Customer Data and/or Personal Data in accordance with this DPA. The preceding authorizations will constitute Customer's prior written consent to the subcontracting by iManage of the Processing of Customer Data and Personal Data if such consent is required.

6.3 Where iManage engages a Sub-Processor for carrying out specific Processing activities on behalf of Customer, the same data protection obligations as set out in this DPA shall be imposed on such Sub-Processor by way of contract or other legal act to the extent required by applicable Data Protection Legislation, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of applicable Data Protection Legislation. Where a Sub-Processor fails to fulfil such data protection obligations, iManage shall remain fully responsible and liable for the performance of such Sub-Processor's obligations.

6.4 Changes to Sub-Processors.

(a) Unless otherwise agreed by the Parties, at least sixty (60) days before authorizing any new Sub-Processor to access Customer Data or Personal Data, iManage shall provide notice of such change by posting to https://support.imanage.com/resources/Subprocessors.htm, which shall have a mechanism allowing Customer to subscribe to notifications of new Sub-Processors. Within thirty (30) days of such notice being posted, Customer may object to the appointment of an additional Sub-Processor on reasonable grounds, provided in writing to iManage, in which case iManage shall have the right to cure the objection through one of the following options (to be selected at iManage's sole discretion):

(1) iManage will cancel its planned use of Sub-Processor or will offer an alternative plan to provide the Services without using such Sub-Processor;
(2) iManage will take the corrective steps, if any, identified by Customer in its objection as sufficient to remove Customer's objection, and proceed to use the Sub-Processor; or
(3) iManage may cease to provide, or Customer may agree not to use (temporarily or permanently), the particular aspect of the Services that would involve the use of such Sub-Processor, subject to a mutual agreement of the Parties to adjust the remuneration for the Services considering the reduced scope of the Services.

(b) If none of the above options are reasonably available or the objection otherwise has not been resolved to the mutual satisfaction of the Parties within thirty (30) days after iManage's receipt of Customer's objection pursuant to this DPA, either Party may terminate the Agreement and Customer will be entitled to a pro-rata refund for prepaid Fees for Services not performed as of the date of termination.

6.5 Emergency Replacement of a Sub-Processor. iManage may replace a Sub-Processor at any time if the need for the change is urgent and necessary, and the reason for the change is beyond iManage's reasonable control. In

such instance, iManage shall notify Customer of the replacement Sub-Processor as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-Processor pursuant to **paragraph 6.4** above. Customer will not be entitled to any remuneration or accrue any rights of termination due to the emergency replacement.

7. Cooperation.

7.1 Requests from Data Subjects.

(a) iManage will assist the Customer, in a manner consistent with the functionality or performance of the Services and iManage's role as a Processor, in respect of any Data Subject requests to exercise one or more of their rights under applicable Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any costs arising from iManage's provision of such assistance beyond the existing functionality or performance of the Services.

(b) If iManage receives a request from one of Customer's Data Subjects to exercise one or more of its rights under applicable Data Protection Legislation, iManage will instruct the Data Subject to make its request directly to Customer. Customer will be responsible for responding to any such request.

7.2 Supervisory Authorities. iManage shall notify Customer without undue delay if a Supervisory Authority makes any inquiry or request for disclosure regarding Personal Data provided by Customer to iManage.

7.3 Other Cooperation. Taking into account the nature of Processing and the information available to iManage, iManage shall provide reasonable assistance to Customer in ensuring compliance with obligations:

(a) to ensure an appropriate level of security;

(b) in cases of a Security Incident, to provide appropriate notifications to Supervisory Authorities and Data Subjects, in accordance with applicable Data Protection Legislation;

(c) where required under applicable Data Protection Legislation, to carry out assessments of the impact of envisaged Processing operations on the protection of Personal Data;

(d) where required under applicable Data Protection Legislation, to consult with Supervisory Authorities with regard to matters related to such Processing; and

(e) to demonstrate compliance with the obligations concerning Processing of Personal Data carried out on behalf of a Controller and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer pursuant to **paragraph 9.1** below.

8. Retention and Deletion of Customer Data and Personal Data.

8.1 Personal Data. Subject to **paragraph 8.2**, iManage shall delete or return Personal Data in accordance with the mutual agreement of the Parties save to the extent that iManage is required by any applicable Law to retain some or all of the Personal Data. In such event, iManage shall extend the protections of the Agreement and this DPA to such retained Personal Data and limit any further Processing of such Personal Data only to those limited purposes for which, and only for so long as, such retention is required by applicable Law.

8.2 Cloud Services. At all times during the applicable Order Term, Customer shall have the ability to access, extract, and delete Customer Data. iManage will retain Customer Data stored in the Cloud Services for ninety (90) days after expiration or termination of Customer's subscription so that Customer may extract Customer Data. After said 90-day period ends, iManage will disable Customer's account and delete all Customer Data (within thirty (30) days) and, where required by Law, shall certify to Customer that it has done so, save to the extent that iManage is required by any applicable Law to retain some or all of such Customer Data. In such event, iManage shall extend the protections of the Agreement and this DPA to such retained Customer Data and limit any further Processing of such Customer Data only to those limited purposes for which, and only for so long as, such retention is required by applicable Law. Nothing contained herein shall require iManage to alter, modify, delete, or destroy backups or other media created in the ordinary course of business for purposes of disaster recovery and business continuity, so long as such backups or other media are kept solely for such purposes and are overwritten, recycled, or otherwise remediated in the ordinary course of business and, in any event, not longer than ninety (90) days after creation. iManage has no liability for the deletion of any data, including Customer Data and Personal Data as described in this **paragraph 8**.

9. Security Reports, Audits and Records.

9.1 Security Reports and Audits.

(a) To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Legislation cannot reasonably be satisfied through (i) audit reports provided by iManage, (ii) documentation, or (iii) other compliance information that iManage makes generally available to its customers, iManage will, not more than one time per calendar year, promptly respond to Customer's audit requests. Before the commencement of an audit, Customer and iManage will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit iManage to unreasonably delay performance of the audit. To the extent needed to perform the audit, iManage will make the processing systems, facilities and supporting documentation relevant to the Processing of Customer Data and Personal Data by iManage, its Affiliates, and its Sub-Processors (where possible) available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to iManage (not less than twenty days), and subject to reasonable confidentiality and security procedures. Neither Customer nor the auditor shall have access to any data from iManage's other customers or to iManage systems or facilities not involved in the Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time iManage expends for any such audit, in addition to the rates for services performed by iManage. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with iManage and iManage shall promptly cure any material non-compliance.

(b) If the Standard Contractual Clauses apply, then this paragraph is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this paragraph varies or modifies the Standard Contractual Clauses or affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses or Data Protection Legislation.

9.2 Records of Processing Activities. iManage shall maintain, to the extent and in the manner required by applicable Data Protection Legislation, a record of all categories of Processing activities carried out on behalf of Customer and, to the extent applicable to the Processing of Personal Data on behalf of Customer, make such record available to Customer upon request.

10. Obligations of Customer.

10.1 Customer acknowledges that: (a) Customer will comply with all applicable Data Protection Legislation (including its obligations thereunder); (b) Customer is responsible for determining whether the Cloud Services are appropriate for storage and Processing of Customer Data and Personal Data; (c) Customer has the right to transfer, or provide access to, Customer Data and Personal Data to iManage and its Sub-Processors for Processing in accordance with the terms of the Agreement and this DPA; (d) Customer is solely responsible for fulfilling any third-party notification obligations related to a Security Incident; and (e) Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject, including, without limitation, those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Legislation.

10.2 Customer Data Sharing. The Cloud Services may enable Authorized Users to share Customer Data or invite third-party users to use and access the Cloud Services. Such third-party users may access, view, download, and share Customer Data. Customer understands and agrees that: (a) it is solely Customer's and its Authorized Users' choice to share Customer Data; (b) iManage cannot control third parties with whom Customer or Authorized Users have shared Customer Data; and (c) Customer and/or its Authorized Users are solely responsible for their sharing of any Customer Data through the Cloud Services.

11. Modification, Supplementation, and Term.

11.1 iManage may modify or supplement this DPA, with notice to Customer, (a) if required to do so by a Supervisory Authority or other government or regulatory entity, (b) if necessary to comply with applicable Data Protection Legislation, (c) to implement Standard Contractual Clauses, or (d) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR or analogous provisions of other applicable Data Protection Legislation. In the event that such required modification or supplement results in Customer becoming non-compliant with Law that is applicable to Customer, Customer may terminate the Agreement (and any impacted Order(s)), and Customer will be entitled to a pro-rata refund for prepaid Fees for Services not performed as of the date of termination.

11.2 This DPA is effective upon Customer's use of the Services for which iManage is a Processor or Sub-Processor.

11.3 This DPA shall remain in force as long as iManage Processes Customer Data or Personal Data on behalf of Customer.

12. Transfers of Customer Data and Personal Data and Location.

12.1 Customer acknowledges that iManage and its Sub-Processors may Process Customer Data and Personal Data in countries that are outside of the European Economic Area ("**EEA**") and the United Kingdom, including, but not limited to, the United States. This will apply even where Customer has agreed with iManage to host Customer Data in the EEA or the United Kingdom, if such Processing is necessary to provide support-related or other services requested by Customer.

12.2 iManage will abide by the requirements of the Data Protection Legislation regarding the collection, use, transfer, retention, and other Processing of Personal Data from the EEA and the United Kingdom. All transfers of Personal Data to a third country or an international organization (including any relevant Sub-Processor) that does not ensure an adequate level of protection will be subject to appropriate safeguards as described in Article 46 of the GDPR and UK GDPR, and such transfers and safeguards will be documented according to Article 30(2) of the GDPR or UK GDPR (as applicable).

12.3 All transfers of Customer Data and Personal Data out of the EEA and the United Kingdom shall be governed by the Standard Contractual Clauses, except for transfers (a) to and from any country which has a valid adequacy decision from the European Commission or the UK Government (as applicable), or (b) to and from any organization which ensures an adequate level of protection in accordance with the applicable Data Protection Legislation. Subject to the foregoing and where indicated as applicable in **Schedule 1** of this DPA, execution of an Order, or this DPA, by Customer includes execution of the Standard Contractual Clauses. In the event any Standard Contractual Clauses include a transition period for implementation, iManage shall ensure the updated Standard Contractual Clauses shall be implemented prior to the expiration of such transition period (including in respect of transfers to any Sub-Processors which rely on the Standard Contractual Clauses).

12.4 Location of Customer Data. All Customer Data shall be stored in the geographic region set forth in the applicable Order. Customer acknowledges that iManage may provide the Services from regions other than those set forth in the applicable Order, including but not limited to, the United States, the United Kingdom, Canada, Australia, and/or India and, thus, iManage Personnel in such locations may have access to Customer Data. Notwithstanding the foregoing, iManage does not control or limit the region or regions from, in, or to which Customer or Authorized Users may access, move, store or otherwise Process Customer Data.

13. California Consumer Privacy Act (CCPA).

13.1 If iManage is Processing Personal Data within the scope of the CCPA ("**CCPA Data**"), iManage makes the following additional commitments to Customer. iManage will Process CCPA Data on behalf of Customer and, not retain, use, or disclose CCPA Data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will iManage "sell" or "share" (as those terms are defined in the CCPA) any CCPA Data. iManage (a) will not combine CCPA Data that iManage receives from, or on behalf of, Customer with personal information that iManage receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, provided that iManage may combine CCPA Data to perform any business purpose as defined in regulations adopted pursuant to the CCPA; (b) grants Customer the right to take reasonable and appropriate steps to help ensure that iManage uses CCPA Data in a manner consistent with Customer's obligations under the CCPA; (c) shall notify Customer in the event that iManage determines it can no longer meet its obligations under the CCPA; and (d) grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of CCPA Data.

14. HIPAA Business Associate.

14.1 If Customer is a "covered entity" or a "business associate" and provides "protected health information" (as those terms are defined in 45 CFR § 160.103) to iManage, the HIPAA Business Associate Agreement attached hereto as **Schedule 2** of this DPA is incorporated by reference into this DPA and the Agreement.

15. Family Educational Rights and Privacy Act.

15.1 If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act ("**FERPA**") apply, iManage agrees to abide by the applicable limitations and requirements imposed by 34 CFR 99.33(a).

16. Miscellaneous.

16.1 iManage and its Affiliates have appointed a data protection officer, EU representative, and UK representative. iManage EMEA Limited acts as iManage LLC's UK representative. The data protection officer may be reached at dpo@imanage.com. Details of the EU representative can be found within iManage's privacy notice at https://imanage.com/about/privacy-notice/.

16.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

16.3 To the fullest extent permitted by Law, any claims brought under this DPA and/or the Standard Contractual Clauses shall be subject to the terms and conditions of the Agreement, including but not limited to, any applicable exclusions and limitations set forth therein. For the sake of clarity, iManage's aggregate liability arising out of this DPA and/or the Standard Contractual Clauses shall in no event exceed the limitations set forth in the Agreement.

Schedule 1 to Data Protection Agreement

Standard Contractual Clauses

The Parties agree that the applicable Standard Contractual Clauses are incorporated into the DPA by reference, as if they had been set out in full, and are populated as follows. Unless expressly stated below, any optional clauses contained within the Standard Contractual Clauses shall not apply.

The following Standard Contractual Clauses shall apply where Personal Data is transferred to a third country (unless the transfer is permitted on the basis of an adequacy decision):

a) CONTROLLER → PROCESSOR (**Module Two**) ("**Controller to Processor Standard Contractual Clauses**") if Customer, acting as a Controller, is making a restricted transfer of Personal Data subject to the GDPR and/or the UK GDPR (as applicable) to iManage, acting as a Processor;

b) PROCESSOR → PROCESSOR (**Module Three**) ("**Processor to Processor Standard Contractual Clauses**") if Customer, acting as a Processor, makes a restricted transfer of Personal Data subject to the GDPR and/or the UK GDPR (as applicable) to iManage acting as a Processor; and/or

c) PROCESSOR → CONTROLLER (**Module Four**) ("**Processor to Controller Standard Contractual Clauses**") if iManage, acting as a Processor, makes a restricted transfer of Personal Data subject to the GDPR and/or the UK GDPR (as applicable) to Customer, acting as a Controller.

UK Addendum

The Parties agree that the UK Addendum is incorporated into the DPA by reference, as if it had been set out in full, and is populated and shall be read against the EU SCCs as follows. Unless expressly stated below, any optional clauses contained within the UK Addendum shall not apply.

Start Date

The UK Addendum is effective from the effective date of the Agreement.

1. Table 1: Parties

Exporter and key contact: As set out in Annex 1 of the Standard Contractual Clauses below.

Importer and key contact: As set out in Annex 1 of the Standard Contractual Clauses below.

2. Table 2: Selected SCCs, Modules and Clauses

As applicable, Module 2, Module 3 or Module 4 of the EU SCCs as incorporated by reference into Schedule 1 of this DPA including any supplementary clauses set out within Schedule 1 of this DPA.

3. Table 3: Appendix Information

As set out in Annex 1 and Annex 2 of the of the Standard Contractual Clauses below.

4. Table 4: Ending this Addendum when the Approved Addendum Changes

In the event the Information Commissioner's Office issues a revised Approved Addendum, in accordance with Section 18 of the UK Addendum which as a direct result of such changes has a substantial, disproportionate and demonstrable increase in: (a) the data importer's direct costs of performing its obligations under the Addendum; and/or (b) the data importer's risk under the Addendum, the data importer may terminate this UK Addendum on reasonable written notice to the data exporter in accordance with Table 4 and paragraph 19 of the UK Addendum.

Supplementary clauses for Module Two and Module Three:

Erasure and deletion: For the purposes of Clause 8.5, Section II of Module Two and Module Three of the Standard Contractual Clauses the data importer shall delete the Personal Data in accordance with **paragraph 8.1** of the DPA.

Audit: The Parties acknowledge that the data importer complies with its obligations under Clause 8.9, Section II of Module Two and Module Three of the Standard Contractual Clauses by (i) acting in accordance with **paragraph 9.1** of the DPA and (ii) exercising its contractual audit rights it has agreed with its Sub-Processors. For the purposes of Clause 8.9(e), Section II of Module Three of the Standard Contractual Clauses, the data exporter shall ensure the results are provided to the relevant controller(s) on a confidential basis and that the controller(s) have committed themselves to confidentiality in respect of the same.

Notifications: For the purposes of Clause 8, Section II of Module Three of the Standard Contractual the data exporter shall use all reasonable endeavors to ensure any instructions provided by the relevant controller(s) are directed via the data exporter. The data exporter shall be responsible for ensuring any notifications provided by the data importer are promptly notified to the relevant controller(s) in order to fulfil the data importer's notification obligations pursuant to Clause 8.

Sub-Processors: For the purposes of Clause 9, Section II of Module Two and Module Three of the Standard Contractual Clauses, the Parties agree that option 2: general written authorization shall apply, and the data importer shall notify the data exporter of any changes in accordance with **paragraph 6** of the DPA. For the purposes of Clause 9, Section II of Module Three of the Standard Contractual Clauses, the data importer shall notify the data exporter of any changes to a Sub-Processor and the data exporter shall be responsible for ensuring such notifications are provided to the relevant controller(s) and shall inform the data importer of any objections within the time frames specified. Copies of any Sub-Processor agreements (redacted as appropriate) requested from the data importer shall be provided to the data exporter for onward provision to the relevant controller, as applicable.

Data Subject Rights: For the purposes of Clause 10(a) to (c) Section II of Module Three of the Standard Contractual Clauses, the Parties acknowledge that given the nature of the Processing by the data importer it would not be appropriate for the data importer to notify or assist the controller directly in respect of any requests received from a Data Subject.

Transfer impact assessment: For the purposes of Clause 14(c), Section III of Module Two and Module Three of the Standard Contractual Clauses, the data exporter acknowledges that iManage may transfer Personal Data to the countries listed at https://support.imanage.com/resources/Subprocessors.htm. The data exporter acknowledges a transfer impact assessment has been made available by the data importer on or prior to the date of the Agreement which the data exporter accepts as sufficient to fulfil the data importer's obligations pursuant to Clause 14(c) and 14(a) of the Standard Contractual Clauses.

For the purposes of Clause 14(c), 15.1(b) and 15.2, Section III of Module Two and Module Three of the Standard Contractual Clauses, the Parties agree that "best efforts" and the obligations of the data importer under clause 15.2 shall mean exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a leading practice engaged in a similar type of undertaking under the same or similar circumstances and shall not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

Governing law and Jurisdiction: For the purposes of Clause 17 and 18, Section IV of Module Two and Module Three of the EU SCCs, the Parties agree that the laws and courts of the Republic of Ireland will apply. For the purpose of the UK Addendum, the Parties acknowledge and accept that the laws and courts of England and Wales will apply.

Supplementary clauses for Module Four:

Erasure and Deletion: For the purposes of Clause 8.1(d), Section II of Module Four of the Standard Contractual Clauses, the data exporter shall delete the Personal Data in accordance with **paragraph 8.1** of the DPA.

Governing law and Jurisdiction: For the purposes of Clauses 17 and 18, Section IV of Module Four of the EU SCCs and the UK Addendum, the Parties agree that the laws and courts of England and Wales will apply.

Annex 1 to the Standard Contractual Clauses (Module Two and Module Three)

A. List of Parties

Data exporter: Customer is the data exporter. The data exporter is a user of the Services.

The data exporter's data protection contact (and EU/UK representative if applicable) is as detailed in the Order or as otherwise provided to the data importer.

Data importer: The data importer is the iManage entity identified in the applicable Order. The data importer provides the Services.

The data importer's data protection contact details are as specified in the DPA.

B. Description of Transfer

Data Subjects: The categories of Data Subjects whose Personal Data may be Processed in connection with the Services are determined and controlled by data exporter in its sole discretion and may include but are not limited to: data exporter's representatives and end users, such as employees, contractors, collaborators, and customers, customers and prospects of data exporter, and employees or contractors of data exporter's prospects and customers.

Categories of data: The categories of Personal Data are determined by data exporter in its sole discretion and may include but are not limited to: first and last name, employer, role, professional title, and contact information (e.g., email, phone, physical address).

Special categories of data: Special categories of Personal Data, if any, are determined by data exporter in its sole discretion and may include, but are not limited to, information revealing racial or ethnic origin, political, religious, or philosophical beliefs, trade union membership or health data.

Frequency, duration, and retention: The Personal Data is transferred on a continuous basis determined by the data exporter. The data importer will Process the Personal Data for the duration of the Agreement and will retain the Personal Data in accordance with **paragraph 8.1** of the DPA.

Nature and purpose of the Processing: iManage will Process Customer Data and Personal Data only as described and subject to the limitations herein (a) to provide Customer the Services in accordance with the Documented Instructions, and (b) for business operations incident to providing the Services to Customer, which may include (i) delivering functional capabilities as licensed, configured, and used by Customer and its Authorized Users, (ii) preventing, detecting, and repairing problems, including Security Incidents, and (iii) providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.

Sub-Processors: Any Sub-Processor appointed by the data importer will Process the Personal Data to assist the data importer in providing the Services as described above for the duration of the Agreement.

C. Competent Supervisory Authority:

The competent Supervisory Authority shall be detailed in the relevant Order or otherwise determined in accordance with Clause 13, Section II of Module Two and Module Three of the EU SCCs. In respect of the UK Addendum, the competent supervisory shall be read as Information Commissioner.

Annex 1 to the Standard Contractual Clauses (Module Four)

A. List of Parties

Data exporter: The data exporter is the iManage entity identified in the applicable Order. The data exporter provides the Services.

The data exporter's data protection contact details are as specified in the DPA.

Data importer: Customer is the data importer. The data importer is a user of the Services.

The data importer's data protection contact (and EU/UK representative if applicable) is as detailed in the Order or as otherwise provided to the data exporter.

B. Description of Transfer

Data Subjects: The categories of Data Subjects whose Personal Data may be Processed in connection with the Services are determined and controlled by data importer in its sole discretion and may include but are not limited to: data importer's representatives and end users, such as employees, contractors, collaborators, and customers, customers and prospects of data importer, and employees or contractors of data importer's prospects and customers.

Categories of data: The categories of Personal Data are determined by data importer in its sole discretion and may include but are not limited to: first and last name, employer, role, professional title, and contact information (e.g., email, phone, physical address).

Special categories of data: Special categories of Personal Data, if any, are determined by data importer in its sole discretion and may include, but are not limited to, information revealing racial or ethnic origin, political, religious, or philosophical beliefs, trade union membership or health data.

Frequency, duration, and retention: The Personal Data is transferred on a continuous basis determined by the data importer. The data exporter will Process the Personal Data for the duration of the Agreement and will retain the Personal Data in accordance with **paragraph 8.1** of the DPA.

Nature and purpose of the Processing: iManage will Process Customer Data and Personal Data only as described and subject to the limitations herein (a) to provide Customer the Services in accordance with the Documented Instructions, and (b) for business operations incident to providing the Services to Customer, which may include (i) delivering functional capabilities as licensed, configured, and used by Customer and its Authorized Users, (ii) preventing, detecting, and repairing problems, including Security Incidents, and (iii) providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.

Sub-Processors: Any Sub-Processor appointed by the data exporter will Process the Personal Data to assist the data exporter in providing the Services as described above for the duration of the Agreement.

Annex 2 to the Standard Contractual Clauses

Security measures implemented by the data importer

The data importer has implemented and will maintain the following security measures intended to protect Customer Data and Personal Data (in conjunction with the security measures described in **Exhibit B** to the Agreement related to solely to Customer Data) against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The security measures set forth in **Exhibit B** to the Agreement are hereby incorporated into this Annex 2 by this reference and are binding on the data importer as if they were set forth in this Annex 2 in their entirety.

Security Measure	Practices
Pseudonymisation and Encryption	**Encryption**. iManage encrypts Customer Data at rest within the Cloud Services using ciphers at least as strong as 256-bit AES. Customer Data in transit to and from the Cloud Services is transferred to/from the Cloud Services across encrypted network connections and/or protocols (i.e., HTTPS and/or VPN). Backups of Customer Data are encrypted and stored in a secondary data center. **Key Management**. iManage provides Customer the opportunity to choose whether iManage or Customer controls the encryption key related to Customer Data.
Ongoing Confidentiality, Integrity, Availability and Resilience	**Standards**. Commercially reasonable and appropriate methods and safeguards are utilized to protect the confidentiality, availability, and integrity of Customer Data and Personal Data. **Confidentiality**. iManage ensures that iManage Personnel authorized to access Customer Data and Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. **Training**. All iManage Personnel with access to Customer Data and Personal Data receive annual training. **Backups**. 24/7 managed backup services are provided that include Customer Data stored in the primary site backed up on at least a daily basis to a secondary site. iManage provides backup services for all components of the solution included in the Cloud Services. Backups are maintained for a period of ninety days in the primary data center, and ninety days in the secondary data center. **Disaster Recovery**. iManage maintains disaster recovery capabilities designed to minimize disruption to the Cloud Services. Included within these plans is disaster recovery incident management, procedures for the recovery of access to Customer Data in the secondary data center, as well as the periodic testing/exercising of the disaster recovery plan.
Regularly Testing, Assessing and Evaluating the Effectiveness of the Measures	**Vulnerability Testing**. iManage conducts vulnerability testing of the Cloud Services on a monthly basis. **Penetration Testing**. iManage undergoes penetration testing of the Cloud Services, conducted by an independent third-party organization, on an annual basis.
User Identification and Authorization	**Access Policy**. An access control policy (physical, technical, and administrative) based on least privileges principles is enforced. **Access Authorization**. • An authorization management system is maintained and designed to ensure that only authorized iManage Personnel (technical and non-technical) are granted access to systems containing Customer Data and Personal Data. • iManage Personnel accessing systems containing Customer Data and Personal Data have a separate, unique username. • Access to Customer Data and Personal Data is restricted solely to iManage Personnel who have a need to access such Customer Data or Personal Data in connection with the Services or as otherwise required by applicable Law. **Authentication**.

Security Measure	Practices
	• Industry standard practices, including strong authentication, are utilized to identify and authenticate all iManage Personnel who attempt to access the iManage network or information systems. • iManage ensures that access rights are revoked for all iManage Personnel immediately upon the termination of their employment, contractual or other relationships with iManage.
Protection of Customer Data During Transmission	**Encryption**. Customer Data in transit to and from the Cloud Services is transferred to/from the Cloud Services across encrypted network connections and/or protocols (i.e., hypertext transfer protocol secure (HTTPS) and/or virtual private network (VPN)).
Protection of Customer Data During Storage	**Encryption**. Customer Data at rest within the Cloud Services is encrypted using ciphers at least as strong as 256-bit advanced encryption standard (AES). **Encryption of Backups**. Backups of Customer Data are encrypted and stored in a secondary data center.
Physical Security	**Security Safeguards**. Physical security safeguards are maintained at any facilities where iManage hosts Customer Data or Personal Data. Physical access to such facilities is only granted following a formal authorization procedure and access rights are reviewed periodically. **Facilities**. Such facilities are rated as Tier 3 data centers or greater, and access to such facilities must be limited to identified and authorized individuals. Such facilities use a variety of industry standard systems to protect against loss of Customer Data and Personal Data due to power supply failure, fire, and other natural hazards.
Event Logging	**Network Security**. iManage utilizes an enterprise-class security information and event management (SIEM) system and maintains firewalls and other control measures (e.g., security appliances, network segmentation) to provide reasonable assurance that access from and to its networks is appropriately controlled. **Event Logging**. iManage logs access and use of information systems containing Customer Data.
System Configuration	**Malicious Software**. Anti-malware controls are maintained to help prevent malicious software from causing accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. **Asset Inventory**. Asset inventories of computing equipment and media used in connection with the processing of Customer Data are maintained. Access to such inventories is restricted to authorized iManage Personnel.
Governance and Management	**Information Security Management**. • iManage has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. • iManage maintains an information security program designed to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. **iManage Personnel**. iManage maintains written policies and procedures that address the roles and responsibilities of iManage Personnel, including both technical and non-technical personnel, who have access to Customer Data and Personal Data in connection with providing the Services. **Data Management**. iManage maintains commercially reasonable controls for information governance and data management in connection with the Cloud Services.
Certification of Processes	**Standards**. iManage adheres, and at all times will adhere, to information security practices at least as protective of Customer Data as identified in ISO 27001 and ISO 27017 (or

Security Measure	Practices
	substantially equivalent or replacement standards) or other generally accepted authoritative standards (e.g., SSAE 16, SOC2). **Independent Assessments**. On an annual basis, iManage has an independent third-party organization conduct an independent assessment of security standards. A business continuity plan is maintained that is compliant with ISO 22301.
Data Minimization / Data Quality	**Data Minimization**. iManage shall make reasonable efforts to use the minimum necessary Customer Data and Personal Data to provide the Services. **Data Quality**. At all times during the applicable Order Term, Customer shall have the ability to amend and delete Customer Data to assist the Customer with its data minimization and data quality obligations.
Data Retention	**Data Retention**. iManage will retain Customer Data stored in the Cloud Services for ninety (90) days after expiration or termination of Customer's subscription so that Customer may extract Customer Data. After said 90-day period ends, iManage will disable Customer's account and delete all Customer Data and Personal Data (within thirty (30) days) and, where required by Law, shall certify to Customer that it has done so, save to the extent that iManage is required by any applicable Law to retain some or all of such Customer Data.
Accountability	**Accountability**. iManage defines accountability as holding individuals accountable for their internal control responsibilities. **Control Activities**. Specific control activities that iManage has implemented in this area are described below. • An employee sanction procedure is in place and documented to communicate that an employee may be terminated for noncompliance with a policy and/or procedure; and • A performance review of employees is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and hold them accountable for their internal control responsibilities.
Portability and Erasure	**Portability**. At all times during the applicable Order Term, Customer shall have the ability to access, extract, and delete Customer Data. **Erasure**. iManage destroys, deletes, or otherwise makes irrecoverable Customer Data upon the disposal or removal of storage media. Customer Data for each Customer is logically separated from data of other iManage customers.

Schedule 2 to Data Protection Agreement

HIPAA Business Associate Agreement

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data, Professional Services Data, or Support Data, the terms of this HIPAA Business Associate Agreement ("**BAA**") shall be incorporated into the Agreement. If there is any conflict between a provision in this BAA and a provision in the Agreement, this BAA will control.

1. Definitions. Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement.

"**Breach Notification Rule**" means the Breach Notification for Unsecured Protected Health Information Final Rule.

"**Business Associate**" shall have the same meaning as the term "business associate" in 45 CFR § 160.103 of HIPAA.

"**Covered Entity**" shall have the same meaning as the term "covered entity" in 45 CFR § 160.103 of HIPAA.

"**HIPAA**" collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health ("**HITECH**") Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

"**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information.

"**Protected Health Information**" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is received by iManage from, or created, received, maintained, or transmitted by iManage on behalf of, Customer through iManage's provision of the Services.

"**Security Rule**" means the Security Standards for the Protection of Electronic Protected Health Information.

2. Permitted Uses and Disclosures of Protected Health Information.

2.1 Performance of the Agreement. Except as otherwise limited in this BAA, iManage may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Agreement; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted under **paragraph 2.2** below.

2.2 Management, Administration, and Legal Responsibilities. Except as otherwise limited in this BAA, iManage may Use and Disclose Protected Health Information for the proper management and administration of iManage and/or to carry out the legal responsibilities of iManage, provided that any Disclosure may occur only if: (a) Required by Law; or (b) iManage obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies iManage of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Responsibilities of the Parties with Respect to Protected Health Information.

3.1 iManage's Responsibilities. To the extent iManage is acting as a Business Associate, iManage agrees to the following:

(a) Limitations on Use and Disclosure. iManage shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. iManage shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA. iManage shall not use Protected Health Information for any advertising, Marketing, or similar commercial purpose of iManage or any

third party. iManage shall not violate the HIPAA prohibition on the sale of Protected Health Information. iManage shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.

(b) Safeguards. iManage shall: (i) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in this BAA; and (ii) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

(c) Reporting. iManage shall report to Customer: (i) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which iManage becomes aware; (ii) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents (as defined below) and no further notice of such Unsuccessful Security Incidents shall be given; and/or (iii) any Breach of Customer's Unsecured Protected Health Information that iManage may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made in accordance with paragraph 5 of **Exhibit C** to the Agreement. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with iManage's and Customer's legal obligations.

For purposes of this paragraph, "**Unsuccessful Security Incidents**" mean, without limitation, pings, and other broadcast attacks on iManage's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. iManage's obligation to report under this paragraph is not and will not be construed as an acknowledgement by iManage of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

(d) Subcontractors. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, iManage shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of iManage to agree in writing to: (i) the same or more stringent restrictions and conditions that apply to iManage with respect to such Protected Health Information; (ii) appropriately safeguard the Protected Health Information; and (iii) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. iManage remains responsible for its Subcontractors' compliance with obligations in this BAA.

(e) Disclosure to the Secretary. iManage shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer's compliance with HIPAA, subject to attorney-client and other applicable legal privileges.

(f) Access. The Parties acknowledge and agree that iManage does not maintain Protected Health Information in a Designated Record Set for Customer. In the event that there is a change in the Services that iManage provides to Customer such that iManage commences maintaining Protected Health Information in a Designated Record Set, then iManage, at the request of Customer, shall within fifteen (15) days make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.

(g) Amendment. Subject to **paragraph 3.1(f)** above, if iManage maintains Protected Health Information in a Designated Record Set for Customer, then iManage, at the request of Customer, shall within fifteen (15) days make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.

(h) Accounting of Disclosure. iManage, at the request of Customer, shall within thirty (30) days make available to Customer such information relating to Disclosures made by iManage as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

(i) Performance of a Covered Entity's Obligations. To the extent iManage is to carry out a Covered Entity obligation under the Privacy Rule, iManage shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

3.2 Customer Responsibilities.

(a) No Impermissible Requests. Customer shall not request iManage to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

(b) Customer Notification Obligations. Customer shall notify iManage of any (i) limitation(s) in the notice of privacy practices of a Covered Entity under HIPAA, to the extent that such limitation may affect iManage's use or

disclosure of Protected Health Information; (ii) changes in, or revocation of, the permission by an Individual to use or disclose their Protected Health Information, to the extent that such changes may affect iManage's use or disclosure of Protected Health Information; and (iii) restriction on the use or disclosure of Protected Health Information that a Covered Entity has agreed to or is required to abide by under HIPAA, to the extent that such restriction may affect iManage's use or disclosure of Protected Health Information.

(c) Contact Information for Notices. Customer hereby agrees that any reports, notification, or other notice by iManage pursuant to this BAA may be made electronically. Customer shall provide contact information on the iManage support website found at https://help.imanage.com (or such other location or method of updating contact information as iManage may specify from time to time) and shall ensure that Customer's contact information remains up to date during the term of this BAA. Failure to submit and maintain as current the aforementioned contact information may delay iManage's ability to provide Breach notification under this BAA.

(d) Safeguards and Appropriate Use of Protected Health Information. Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer's obligation to not include Protected Health Information in: (i) information Customer submits to technical support personnel through a technical support request or to community support forums; or (ii) Customer's address book or directory information.

4. Applicability of BAA. This BAA is applicable to only the Services.

5. Term and Termination.

5.1 Term. This BAA shall continue in effect until the earlier of (a) termination by a Party for breach as set forth in **paragraph 5.2** below, or (b) expiration or termination of the Agreement.

5.2 Termination for Breach. Upon written notice, either Party immediately may terminate the Agreement and this BAA if the other Party is in material breach or default of any obligation in this BAA. Either Party may provide the other a thirty (30) day period to cure a material breach or default within such written notice.

5.3 Return, Destruction, or Retention of Protected Health Information Upon Termination. Upon expiration or termination of this BAA, iManage shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement. If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, then iManage shall extend the protections of this BAA, without limitation, to such Protected Health Information and limit any further Use or Disclosure of the Protected Health Information to those purposes that make the return or destruction infeasible for the duration of the retention of the Protected Health Information.

6. Miscellaneous.

6.1 Interpretation. The Parties intend that this BAA be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except where this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged. Any captions or headings in this BAA are for the convenience of the Parties and shall not affect the interpretation of this BAA.

6.2 Amendment; Waiver. This BAA may not be modified or amended except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.

6.3 No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything in this BAA confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

6.4 Severability. In the event that any provision of this BAA is found to be invalid or unenforceable, the remainder of this BAA shall not be affected thereby, but rather the remainder of this BAA shall be enforced to the greatest extent permitted by law.

6.5 No Agency Relationship. It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Customer and iManage under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render iManage an agent of Customer.