



## SUPPLIER FRAMEWORK AGREEMENT

This Supplier Framework Agreement (this “**Supplier Framework Agreement**”), effective as of **March 31, 2022** (the “**Effective Date**”), is by and between **NTT**, with its principal place of business at **123 Elm Street** “**Supplier**”), and Alight Solutions LLC, with its principal place of business at 4 Overlook Point, Lincolnshire, IL 60069 (“**Alight**” and, together with Supplier, each a “**Party**” and collectively the “**Parties**”). In consideration of the mutual covenants contained herein, and other valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

**Section 1. Contractual Framework.** This Supplier Framework Agreement is a framework arrangement that sets forth terms for each Order (as defined below). This Supplier Framework Agreement does not establish any rights, obligations or liabilities unless, and only to the extent that, the terms of this Supplier Framework Agreement are incorporated into an Order, in which case such terms shall only be binding upon the parties to such Order. An Order may be entered into by the Parties to this Supplier Framework Agreement or any of their respective affiliates, and all references to “Alight”, “Supplier” and “Party(ies)” in this Supplier Framework Agreement shall refer to the applicable entities that entered into such Order for purposes thereof. All references in this Supplier Framework Agreement to the “**Agreement**” shall refer to the Order together with this Supplier Framework Agreement incorporated therein. Each Agreement is a separate and severable agreement between the applicable Parties thereto and each such Party shall be solely responsible for its obligations thereunder.

### Section 2. Orders.

**2.1. Placement of Orders.** Alight, or its affiliates, may place an Order with the Supplier for products, software, or services by referencing this Supplier Framework Agreement. For clarity, as used herein, “**Order**” means a transactional document between the Parties referencing the Supplier Framework Agreement and detailing what Alight is procuring from the Supplier (e.g. a duly executed Order Form, a Statement of Work (“**SOW**”), or purchase quote).

**2.2. Change Orders.** Each Party may request changes to an Order. If the Parties agree to proceed with a change, a written change order (a “**Change Order**”) describing the change (including the impact of the change on work, services, scope, specifications, volumes, licenses, timeline, fees, etc.) shall be prepared by Supplier and submitted to Alight for review. For clarity, if there are Change Orders which result in de minimus changes to an Order, Supplier will not charge Alight additional fees under the Order. Each Party is responsible for its own costs associated with developing a Change Order unless mutually agreed. To be effective and for Supplier to implement such Change Order, each Change Order shall be identified as such and be duly executed (or otherwise approved via another mutually agreed method) by an authorized representative of each Party. Each Change Order shall be deemed an amendment to the Agreement.

### Section 3. Compensation.

**3.1. Fees.** The fees payable in connection with an Order shall be set forth in the applicable Order. Unless specifically stated otherwise in an Order, Alight shall pay all fees within 90 days of receipt of an undisputed invoice. Alight will not be responsible for any fees that are not invoiced within one hundred and eighty (180) days of the delivery of the applicable products, software, or services.

**3.2. Taxes.** Alight will be responsible for and pay any taxes, duties, or other charges, including sales or use taxes, imposed by any federal state, or local governmental entity invoiced by Supplier arising directly out of the Agreement, including VAT taxes where applicable, but excluding any taxes on the Supplier’s taxable income, gross revenue or employment obligations.

**3.3. Expenses.** In order to seek reimbursement for any expenses not otherwise included in the Order, the Supplier must seek and receive approval in writing from Alight prior to incurring such expenses. Any such expenses will be invoiced to Alight at the cost to the Supplier with no mark-up and submitted consistent with Alight’s Expense Guidelines located at <https://alight.com/alightreimbursementguidelines>.

## **Section 4. Term and Termination.**

**4.1. Term; Effect of Termination.** The term of this Supplier Framework Agreement shall begin on the Effective Date and shall continue until terminated by either Party. The termination of this Supplier Framework Agreement shall not result in the termination of any Agreement. The term of any Agreement shall be set forth in the applicable Order. The termination of an Agreement shall not result in the termination of this Supplier Framework Agreement or any other Agreement. The rights and obligations of the Parties which, by their nature, should survive termination or expiration of the Agreement, shall survive such termination or expiration.

**4.2. Termination for Convenience.** The Agreement may be terminated for convenience as provided in the applicable Order.

**4.3. Termination for Cause.** Each Party may terminate an Agreement for cause if the other Party materially breaches the terms of the Agreement and such breach is not cured within 30 days after the non-breaching Party has delivered notice of such breach to the breaching Party. Additionally the Parties agree that if Supplier breaches any Service Level Agreement ("SLA") two (2) times within a five (5) month period, Alight may terminate the Agreement for cause under this Section upon 30 days notice without a right for the Supplier to cure such breaches.

**4.4. Bankruptcy.** Alight may terminate an Agreement immediately and cancel any unfulfilled obligations if the Supplier becomes insolvent, unable to pay its debts as they become due, files for or is subject to bankruptcy or receivership or forced asset assignment.

**Section 5. Supplier Diversity.** Alight seeks to include Diverse Sellers in awarding bids for goods and services and to identify Diverse Sellers, either directly or indirectly. "Diverse Sellers" include businesses that are owned by minorities, women, disabled persons, veterans, disabled veterans, as well as those categorized as small disadvantaged businesses. Diverse Sellers must be certified by a national or regional organization that validates diversity status. To support Alight's supplier diversity goal, Supplier will: (a) provide information about its supplier diversity program and good faith efforts to utilize diverse suppliers or subcontractors in its business; (b) submit quarterly reports within thirty days following each quarter end that identify projects and services furnished by Diverse Sellers to Supplier in direct support of the Alight account, such reports shall be submitted to Alight or its designated provider and (c) document the good faith efforts made during the quarter to increase support of Diverse Sellers, which may include an annual questionnaire regarding such efforts if requested by Alight. If Supplier is certified as a Diverse Seller by a national or regional organization Supplier will provide such certification to Alight and complete or provide all forms and documentation reasonably requested to evidence such qualification and will maintain such forms and documentation.

**Section 6. Record Retention and Audit.** Supplier agrees to maintain accurate books, accounts, and records of its activities under this Supplier Framework Agreement and all Orders for the greater of seven (7) years or the period required by law. Supplier agrees that Alight (or its designated auditors who will themselves be under an obligation of confidentiality) will be entitled to audit the Supplier (and make and retain copies of all records they make) during the Term to verify compliance with the Supplier's obligations under this Supplier Framework Agreement and any Order. Alight will only do so providing it has given reasonable prior notice to Supplier and will endeavor to limit the disruption to the Supplier. The Supplier will provide all reasonable assistance that Alight (or its designated auditors) require in conducting such an audit. The supplier shall be notified at least seven business days in advance of the Audit. In the event such audit identifies Supplier's non-compliance with this Supplier Framework Agreement or any Order, the reasonable cost of such audit shall be to Supplier's account, and Supplier will re-pay to Alight any overpayments identified by the audit. In any circumstance where the Supplier engages a subcontractor to perform any activities under an Order, the Supplier agrees to include an obligation on the subcontractor to comply with Alight audit requests that is no less stringent than what the Supplier agrees to in this Section.

**Section 7. Supplier Personnel.** All Supplier personnel who provide products or services under an Order (including Supplier employees, and contractors) will have the skills and qualifications to perform the Supplier obligations under the Agreement. Supplier will insure that it has performed a pre-employment background check in compliance with local regulations and the principles in (Background Check Requirements) on all Supplier personnel involved in the provision of products, software, or services under the Agreement.

## Section 8. Confidentiality.

**8.1. Confidential Information.** For purposes hereof, “**Confidential Information**” means all information, irrespective of the form thereof, disclosed by or on behalf of either Party (as applicable, the “**Disclosing Party**”) to the other Party (as applicable, the “**Receiving Party**”) or its Representatives (as defined below) in connection with the subject matter hereof that is marked confidential or which otherwise would be understood by a reasonable person in the position of the Receiving Party to be confidential in nature, including any such information regarding the Disclosing Party’s services, Alight Data, products, systems, software, marketing, pricing, operations, financial results, plans, strategies, trade secrets, know-how, methods, Personal Information (as defined below) intellectual property and its relationship with employees, prospects, customers, suppliers and other third parties, as well as the terms of the Agreement; provided, however, that, except for Personal Information (as defined below) (which shall at all times be treated as confidential), “Confidential Information” shall not include any information that (a) is or becomes generally available to the public other than as a result of a disclosure thereof by the Receiving Party or its Representatives in violation hereof, (b) was or becomes available to the Receiving Party from a source other than the Disclosing Party or its Representatives that, to the Receiving Party’s knowledge, was not prohibited from disclosing such information pursuant to a contractual, legal or fiduciary obligation of confidentiality to the Disclosing Party, or (c) is or was independently developed by the Receiving Party or its Representatives without the use of any information that would otherwise be Confidential Information hereunder. “**Personal Information**” means any information processed by or on behalf of Supplier for Alight or Alight’s clients in connection with the Agreement that (a) relates to an identified or identifiable natural person, where an identifiable natural person is one who can be identified, directly or indirectly, from such information alone or in combination with other information processed by or on behalf of Supplier, in particular by reference to an identifier such as a name, an identification number, biometric data, 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, or (b) is otherwise protected under the Data Protection Laws, as defined in Schedule 1 (Data Privacy Agreement).

**8.2. Restrictions.** The Receiving Party shall not release, nor allow the release of, the Disclosing Party’s Confidential Information, and will not use the Disclosing Party’s Confidential Information for any purpose other than to exercise its rights or perform its obligations hereunder. The Receiving Party shall not, without the prior written consent of the Disclosing Party, disclose any of the Disclosing Party’s Confidential Information to any unrelated third party other than the Receiving Party’s affiliates and its and their directors, officers, employees, independent contractors, advisors, subcontractors, vendors, agents or other representatives (collectively, “**Representatives**”) who, in each case, (a) reasonably require access to such Confidential Information to assist the Receiving Party to exercise its rights or perform its obligations under the Agreement and (b) have a contractual, legal, professional or fiduciary obligation of confidentiality to the Receiving Party that is consistent in all material respects with the Receiving Party’s obligations of confidentiality to the Disclosing Party hereunder. The Receiving Party shall be responsible for any use or disclosure of the Disclosing Party’s Confidential Information by any of its Representatives (in their capacity as such) to the extent such use or disclosure, if by the Receiving Party, would not be permitted hereunder.

**8.3. Required Disclosure.** Notwithstanding the foregoing, if the Receiving Party or any of its Representatives is requested or required to disclose any of the Disclosing Party’s Confidential Information by law or legal process, then (a) the Receiving Party shall (if permitted by law) promptly notify the Disclosing Party and reasonably cooperate with the Disclosing Party (at the Disclosing Party’s expense) in its efforts to obtain an appropriate protective order or other remedy and (b) if such protective order or other remedy is not obtained, the Receiving Party or its Representative (as applicable) may disclose that portion of the Confidential Information which is legally required to be disclosed and shall use commercially reasonable efforts to obtain reasonable assurances that confidential treatment, if available, will be accorded such Confidential Information.

**8.4. Obligations on Termination.** Subject to any other obligations herein with respect to the return or retention of information, following termination of the Agreement, the Receiving Party shall, and shall require its Representatives to, destroy all Confidential Information in the possession, or under the control, of the Receiving Party or its Representatives in connection with the Agreement; provided, however, that the Receiving Party and its Representatives shall be entitled to retain copies of Confidential Information to the extent necessary to comply with applicable law, litigation or bona fide records retention purposes, in each case, to the extent permitted by law. Notwithstanding the obligations detailed in this Section,

the Supplier and its Representatives will delete all Personal Information in their possession or control at the end of an Agreement's term.

**8.5. Injunctive Relief.** In addition to any other remedy to which it may be entitled, the Disclosing Party shall be entitled to seek an injunction or other equitable remedy to prevent or enjoin breaches of this Section 8 (Confidentiality) by the Receiving Party or any of its Representatives.

## **Section 9. Proprietary Rights.**

**9.1. Alight Data.** As between the Parties, all right, title and interest, including all intellectual property rights, in and to all information and other materials provided or otherwise made available to Supplier by or on behalf of Alight in connection herewith shall be owned by Alight ("**Alight Data**"). For clarity, all "Data" (as defined below) made available to Supplier by or on behalf of Alight will be Alight Data. Alight hereby grants Supplier a non-exclusive, royalty-free license to use Alight Data solely in connection with Supplier's provision of goods or services within the scope of an Order.

**9.2. Deliverables.** Certain Orders may define reports records, or other tangible outcomes of the services to be provided by or on behalf of Supplier to Alight in performing the services ("**Deliverables**"). Alight shall be the owner of all Deliverables and the Supplier hereby assigns any rights it, or any of its subcontractors, may have in the Deliverables to Alight as a "work made for hire". For clarity, this assignment of rights includes the right of Alight to assign the Deliverables to Alight's clients or Alight's affiliates. If any Deliverables do not constitute a work for hire, then, the Supplier assigns, where relevant, to Alight, with full title guarantee and free from all third party rights, and shall obtain waivers of all moral rights in the Deliverables to which any individual is now or may be at any future time entitled.

**9.3. Supplier Intellectual Property.** As between the Parties, all right, title and interest, including all intellectual property rights, in and to all elements of the services and Deliverables (including all trade names, trade secrets, templates, know-how, methods, software, information and other materials), existing prior to the Effective Date shall be owned by Supplier ("**Supplier IP**"). Supplier hereby grants Alight, and Alight's client's, a non-exclusive, worldwide, perpetual, irrevocable, transferrable, royalty-free license to use Supplier IP to the extent necessary to enable Alight to make reasonable use of the services and Deliverables; including the right to create derivative works based on the Deliverables.

**Section 10. Compliance with Law.** Each Party shall comply in all material respects with the laws applicable to its business, operations and employment of its personnel. Supplier agrees that it will comply with, and insure that all of its personnel comply with Alight's Supplier Code of Conduct detailed in Schedule 4 (Alight Supplier Code of Conduct).

## **Section 11. Data Protection.**

**11.1. Data Privacy.** The Supplier agrees to preserve the confidentiality, integrity and accessibility of any data or other information obtained in their performance under the Agreement ("**Data**") with administrative, technical and physical measures that conform to generally recognized industry standards and best practices, in compliance with all laws concerning data protection and security, and which provide, at minimum, the same level of protection to Alight's Data as it does to its own data of similar character. Maintenance of a secure processing environment includes but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by Supplier or open source support, access controls, log management, rogue device detection, and malicious code protective measures. Supplier's specific data security requirements are detailed in Schedule 1 (Data Privacy Agreement).

**11.2. Business Continuity and Disaster Recovery.** Supplier will maintain during the term of the Agreement a business continuity and business resumption plan that complies with the minimum requirements pursuant to the "Business Continuity Requirements" set forth in Schedule 2 (Business Continuity Requirements) attached hereto and made a part hereof to ensure Supplier's continued performance under this Supplier Framework Agreement and all Orders. For the avoidance of doubt, the Force Majeure Events (as defined below) described in this Supplier Framework Agreement shall not excuse Supplier's performance under the Business Continuity Requirements.

## Section 12. Remedies and Liability.

**12.1. Infringement Indemnity.** Supplier agrees to indemnify, defend and hold harmless Alight, its clients, affiliates, successors and assigns and each of their respective officers, directors, employees and agents (collectively, the “Indemnitees”) from and against any and all claims by third parties for damages, liabilities, penalties, fines, losses, costs and expenses including reasonable attorneys’ fees (collectively, “Losses”) arising from or relating to any claim or allegation that the goods or services procured under this Supplier Framework Agreement or any Order violate, misappropriate or infringe any Intellectual Property Rights, or misappropriate any trade secret, of any third party or violate the terms of any third party software license contained within goods or services procured under this Supplier Framework Agreement or any Order. If any goods or services procured under this Supplier Framework Agreement or any Order, in whole or in part, constitute or may constitute infringement, violation or misappropriation of any third party’s Intellectual Property Rights, and/or if Alight’s use thereof is or may be enjoined, Supplier, in addition to its indemnification obligations hereunder, shall promptly either: (i) secure for Alight rights to continue using such infringing goods or services procured under the Order; or (ii) re-perform or replace such goods or services procured under the Order with comparable non infringing goods or services; or (iii) modify the goods or services procured under the Order so that they become non infringing. In the event Supplier is unable to procure one of the aforementioned remedies, ~~Supplier shall, in addition to its indemnification obligations hereunder, promptly refund to Alight all amounts paid to Supplier under the Order for the goods or services procured under the Order that are the subject of such infringement claim.~~

**12.2. General Indemnification.** Supplier shall indemnify, defend and hold harmless the Indemnitees from and against any and all Losses arising from or relating to the acts or omissions of Supplier, ~~its subcontractors, employees or representatives in their provision of the goods, services software or SAAS under any Order.~~

**12.3. Notification, Rights and Cooperation.** Alight agrees to give Supplier prompt written notice of any claim subject to indemnification; provided that Alight’s failure to promptly notify Supplier shall not affect Supplier’s obligations hereunder except to the extent that Alight’s delay prejudices Supplier’s ability to defend such claim. Supplier shall have the right to defend against any such claim with counsel of its own choosing and to settle such claim as Supplier deems appropriate, provided that Supplier shall not enter into any settlement that adversely affects Alight’s rights without Alight’s prior written consent. ~~Alight agrees to reasonably cooperate with Supplier in the defense and settlement of any such claim, at Supplier’s expense.~~

## Section 13. Limitation. of Liability

**13.1. DISCLAIMER.** EXCEPT FOR THE INDEMNITIES DETAILED IN SECTION 12, BREACHES OF THE CONFIDENTIALITY OBLIGATIONS IN SECTION 8, BREACHES OF THE DATA PRIVACY OBLIGATIONS IN SECTION 11, VIOLATIONS OF THE COMPLIANCE WITH LAW OBLIGATIONS IN SECTION 10, AND THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY CLAIM ARISING UNDER THIS SUPPLIER FRAMEWORK AGREEMENT AND ANY ORDER, REGARDLESS OF THE CAUSE OF ACTION AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## Section 14. Representations and Warranties. Each Party represents and warrants to the other that:

- a) It has all requisite corporate power and authority to undertake and perform its duties and obligations under this Supplier Framework Agreement and all Orders;
- b) It is duly constituted, validly existing and in good standing under the laws of its jurisdiction of formation;
- c) By executing this Supplier Framework Agreement and all Orders, each Party does not violate any other agreement to which it is a party;
- d) They will comply with all applicable laws and regulations related to the provision of the goods and services under this Supplier Framework Agreement and all Orders;
- e) There are no actions, suits, proceedings or investigations in which an adverse decision, ruling or finding against it would impair its ability to perform its duties and obligations under this Supplier Framework Agreement and all Orders; and
- f) It will comply with any warranties detailed in an applicable Order.

**Section 15. Insurance.** At Supplier's sole expense, Supplier will maintain insurance coverage as specified in Schedule 3 (Insurance Requirements) during the Term of this Supplier Framework Agreement and two (2) years thereafter.

**Section 16. Dispute Resolution.** The Parties shall use good faith efforts to resolve any dispute, claim or proceeding arising out of or relating to this Supplier Framework Agreement and all Orders via discussion between their representatives identified in an Order. In the event that any disputes cannot be resolved at this level then the senior executives of the relevant Parties who have authority to settle the dispute shall use good faith efforts to resolve the same.

Nothing contained herein will prevent one Party from seeking injunctive relief for actual or threatened breaches from a court of competent jurisdiction.

**Section 17. Miscellaneous.**

**17.1. Entire Agreement.** The Agreement, together with any Change Order or Order and all exhibits and schedules referenced herein and therein, constitutes the sole and entire agreement of the Parties with respect to the subject matter hereof and thereof, and supersedes all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, with respect to such subject matter

**17.2. Severability.** If any provision of the Agreement, or the application thereof to any person, place or circumstance, shall be held by a court of competent jurisdiction to be invalid, void or unenforceable, the remainder of the Agreement and such provision as applied to other persons, places or circumstances shall remain in full force and effect and such invalid, void or unenforceable provision shall be enforced to the fullest extent permitted by law.

**17.3. Amendment; Waiver.** Neither this Supplier Framework Agreement nor the Agreement may be amended or otherwise modified unless such amendment or modification is set forth in writing, identified as an amendment or modification thereof and duly executed by an authorized representative of each of the applicable Parties. No provision of this Supplier Framework Agreement or the Agreement may be waived unless such waiver is set forth in writing, identified as a waiver thereof and signed by an authorized representative of the waiving Party. An amendment or waiver of this Supplier Framework Agreement shall have no effect on any Agreement in effect at the time of such amendment or waiver unless otherwise agreed by each of the applicable Parties. An amendment or waiver of the Agreement shall have no effect on this Supplier Framework Agreement or any other Agreement. Except as otherwise provided in the Agreement, no failure or delay by a Party in exercising any right under the Agreement shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right.

**17.4. Assignment.** Alight may assign the Supplier Framework Agreement or the Agreement in whole or in part along with any of its rights or obligations under the Supplier Framework Agreement or the Agreement without the consent of the Supplier. The Supplier may not assign this Supplier Framework Agreement or the Agreement (including to any affiliate) without the prior written consent of Alight and any purported assignment without such consent shall be void and unenforceable

**17.5. Sub-Contracting.** Unless Alight approved subcontractors are specifically stated in an Order, or Alight provides specific written approval of a subcontractor, the Supplier may not engage subcontractors or other third parties to perform any portion of the services. Where Alight does approve Supplier's engagement of subcontractors, the Supplier shall remain responsible for the performance of such to the same extent as if such activities under the Agreement were performed by the Supplier

**17.6. No Third Party Beneficiaries.** The Agreement shall be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other person any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of the Agreement.

**17.7. Relationship of the Parties.** The Supplier is an independent contractor of Alight and the Agreement will not establish any agency, partnership, joint venture, fiduciary, franchise or employment relationship between the Parties (or between one Party and the Representatives of the other Party). The Supplier by virtue of the Agreement shall have any right,

power or authority, express or implied, to bind the other Alight. Except for its express obligations hereunder, the method and manner for performance of the services shall be under the exclusive control of Supplier.

**17.8. Choice of Law.** This Supplier Framework Agreement and the Agreement and any dispute or claim arising out of or in connection therewith or the subject matter or formation thereof (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of the state of Illinois without regard to conflict of law principles that would cause the application of the laws of any other jurisdiction. Each Party irrevocably and unconditionally agrees that it will not commence any action, litigation or proceeding of any kind whatsoever against the other Party in any way arising from or relating to this Supplier Framework Agreement or the Agreement or the subject matter or formation thereof (including non-contractual disputes or claims), in any forum other than the nation where Alight's office is located, as set out above and hereby expressly and irrevocably submits to the exclusive personal jurisdiction and venue of such courts for the purposes thereof and expressly waives any claim of improper venue and any claim that such courts are an inconvenient forum.

**17.9. Force Majeure.** Notwithstanding anything to the contrary herein, neither Party shall be liable for, nor be deemed to be in breach hereof as a result of, any failure to comply with its obligations hereunder to the extent attributable to any act of God, flood, fire, earthquake, hurricane, act of war or other hostility, act of terrorism, governmental action or inaction, civil unrest, national emergency, epidemic, strike or other labor dispute, act or omission by a third party or a third party product or service, power, telecommunication or other service outage or any other cause or circumstance beyond the reasonable control of such Party ("**Force Majeure Events**"); provided that nothing in this Section shall limit or otherwise affect Supplier's obligation to execute its business continuity and disaster recovery program. The affected Party shall give the other Party prompt notice of any such event and use commercially reasonable efforts to end and minimize the effects thereof. The Parties shall use commercially reasonable efforts to mitigate the effects of any of the foregoing circumstances.

**17.10. Counterparts.** This Supplier Framework Agreement and each Order may be executed in any number of counterparts, each of which when so executed and delivered shall constitute an original, but such counterparts shall constitute one and the same instrument. This Supplier Framework Agreement and each Order may be executed and delivered electronically.

**17.11. Interpretation.** Unless the express context otherwise requires, the words "hereof", "herein", "hereunder" and words of similar import refer to the Agreement as a whole and not to any particular provision of the Agreement, references to a specific section, exhibit or schedule in this Supplier Framework Agreement or an Order refer to the sections, exhibits or schedules in this Supplier Framework Agreement or such Order (as applicable) unless otherwise expressly provided and the words "include", "including" and words of similar import shall be deemed to be followed by the words "without limitation". Each Change Order and all exhibits and schedules referenced herein or therein are incorporated in and made a part of the Agreement as if set forth in full herein. The captions or headings in the Agreement are for convenience only and shall not be considered a part of or affect the construction or interpretation of any provision of the Agreement.

**17.12. Hierarchy.** If there is a conflict between a term in this Supplier Framework Agreement and a term in any Order, the term in the Order shall control to the extent of any conflict.

**17.13. Most Favored Customer.** During the term of any Agreement, the financial terms of the Agreement will be at least as favorable or more favorable than the financial terms of any other current or prospective Supplier customer that engages Supplier for goods or services substantially similar to the goods and services purchased by Alight under the relevant Agreement.

**17.14. Notices.** All notices under the Agreement shall be in writing and shall be deemed to have been given on the next business day after it is sent, if sent by overnight courier service (provided delivery is confirmed), or when actually received, if sent by other means, in each case, to the address of the applicable Party first written above (in the case of notices to Alight, to the attention of the Legal Dept. as follows:

ATTN: General Counsel  
Alight Solutions, LLC

4 Overlook Point  
Lincolnshire, IL 60069

and to the email address: legalrequests@alight.com) or at such other address as shall be specified in the Agreement or by notice delivered in accordance herewith.

**17.15. Publicity.** The Supplier shall not publicize this Supplier Framework Agreement or any Order. Additionally, The Supplier shall not use in any manner, the name or trademarks of Alight or any Alight affiliate, without the prior written approval of Alight.

\* \* \* \* \*



## Index of Schedules

- Schedule 1: Data Privacy Agreement
- Schedule 2: Business Continuity Requirements
- Schedule 3: Insurance Requirements
- Schedule 4: Alight's Supplier Code of Conduct
- Schedule 5: Background Check Requirements

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

**[SUPPLIER NAME MOURI TECH PRIVATE LIMITED]**

**ALIGHT SOLUTIONS LLC**

By: \_\_\_\_\_

Name:

Title:

Date:

By: \_\_\_\_\_

Name:

Title:

Date:

## SUPPLIER DATA PRIVACY AGREEMENT

This Supplier Data Privacy Agreement ("**DPA**"), effective as of January 7, 2022 (the "**Effective Date**"), is by and between Alight Solutions LLC ("**Alight**"), and EPI - USE, Inc ("**Supplier**" and, together with Alight, each is a "**Party**" and collectively they are the "**Parties**"). This DPA is entered into in connection with services to be provided by Supplier to Alight ("**Services**") under that certain Supplier Framework Agreement, effective as of January 7, 2022, by and between the Parties (the "**SFA**"), pursuant to which Supplier may be required to process Personal Information (as defined below). All references in this DPA to the "**Agreement**", shall refer to the Order (defined in the SFA) inclusive of the terms of the SFA. The Order may also be from time to time identified as a Work Order, Statement of Work or SOW.

In consideration of the mutual covenants contained herein, and other valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

### Section 1. Definitions.

**1.1. "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 European Union or EU Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or EU Member State law.

**1.2. "Data Protection Laws"** means all applicable laws and regulations regarding privacy, security or data protection, including but not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"), the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the Gramm-Leach-Bliley Act ("**GLBA**"), the UK Data Protection Act of 2018 and the New York Department of Financial Services Regulations, and such other state, province and national laws and regulations that may apply,

as any are amended, repealed or replaced. The use of “Data Protection Laws” herein means collectively all, a combination of, or any single, such law or regulation.

**1.3. “Data Subject”** means, with respect to any Personal Information, the subject of such Personal Information.

**1.4. “Personal Information”** means any information or data processed by Supplier that (a) relates to an identified or identifiable natural person, where an identifiable natural person is one who can be identified, directly or indirectly, from such information or data alone or in combination with other information or data processed by or on behalf of Supplier, 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, or (b) is otherwise protected under the Data Protection Laws.

**1.5. “Processing” or “Process(es)”** means (a) any operation or set of operations that are performed on Personal Information or on sets of Personal Information, whether or not by automated means, including collection, storage, adaptation or alteration, retrieval, use, disclosure, erasure or destruction, and (b) any other activity involving Personal Information included in the definition of “processing” under Data Protection Laws.

**1.6. “Processor”** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

**1.7. “Restricted Transfer”** means a transfer of Personal Information from the European Union (“EU”) or the European Economic Area (“EEA”) to any third country not recognized by the European Commission as providing an adequate level of protection.

**1.8. “Standard Contractual Clauses” or “SCCs”** means the EU standard contractual clauses for the transfer of personal data from the EU or the EEA to third countries, or any successor documents or transfer mechanisms. As of the Effective Date, a reference to the SCCs means the applicable module of Commission Implementing Decision (EU) 2021/914.

**1.9. “Subprocessor”** means any person (other than an employee) or other entities, including Supplier’s affiliates, appointed by or on behalf of Supplier to Process Personal Information for or on behalf of Alight.

## **Section 2. Processing Personal Information.**

**2.1. Instructions; Limits on Processing.** Alight hereby appoints and instructs Supplier to Process Personal Information only for the purposes of: providing services, goods or software for or on behalf of Alight; complying with applicable law; and complying with any other instruction provided by or on behalf of Alight (the “Purpose”). The Purpose is a “Business Purpose”, as defined by CCPA. Where Supplier Processes Personal Information *on behalf of* Alight for its clients, Supplier will act as Processor under the instructions of a client of Alight, with the client of Alight being the Controller (Alight shall make the client’s instructions available to the Supplier prior to the Processing). Where Supplier Processes Personal Information *for* Alight, it acts as a Processor of Alight, with Alight being the Controller. Whether Supplier Processes Personal Information *for* or *on behalf of* Alight, it shall only Process Personal Information in accordance with the documented instructions which may be given throughout the duration of the Order. Supplier shall only collect, retain, use, disclose or otherwise Process Personal Information for the Purpose and it shall not sell Personal Information (either as that term is commonly understood, or as “Sell” is defined by CCPA or other Data Protection Laws). Supplier shall immediately notify Alight if, in Supplier’s opinion, an instruction provided by or on behalf of Alight violates any Data Protection Law. Personal Information disclosed to Supplier by or on behalf of Alight will only be provided to Supplier, and Supplier shall only Process Personal Information, for a Business Purpose. Supplier certifies that it understands and will comply with all of the limits on Processing set forth in this Section 2, including this subpart 2.1 and all other subparts of this Section 2. Alight’s

instructions to Supplier will comply with Data Protection Laws and Alight will not and shall not sell Personal Information to Supplier.

**2.2. Limits on Disclosure.** Supplier shall not disclose any Personal Information to any third party except as necessary to fulfill the Purpose and otherwise in accordance with this DPA. If Supplier or any of its representatives is requested or required to disclose or otherwise Process any Personal Information by law or legal process (including judicial authorities), then Supplier shall (if permitted by law) promptly notify Alight and reasonably cooperate in Alight's efforts to obtain an appropriate protective order or other remedy.

**2.2.1.** Such notification shall include, at least, (a) information about the Personal Information requested, (b) the requesting authority, (c) the legal basis for the request and (d) the response provided (if any).

**2.2.2.** If Supplier is or becomes aware of any direct access by public authorities to Personal Information, then Supplier must inform Alight immediately and without undue delay with all information available to the Supplier and shall update Alight at regular intervals if it becomes aware of additional information (if permitted by applicable law).

**2.2.3.** If Supplier is prohibited to notify Alight, in accordance with applicable law, then Supplier agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, and as soon as possible, to Alight. Supplier agrees to document its best efforts in order to demonstrate them upon request of Alight.

**2.2.4.** Supplier shall, under any circumstances, regardless of whether it is permitted or not to notify Alight, review or assess the legality of the request and challenge the request, if it deems that there are reasonable grounds to consider that the request is unlawful under applicable law, and shall seek measures with a view to suspending the effects of the request. Such review or assessment and challenge shall be documented and made available to Alight or the competent authority upon request.

**2.2.5.** Where despite Supplier's best efforts the disclosure of Personal Information cannot be avoided, Supplier shall only provide or disclose the minimum amount of Personal Information when responding to a request for disclosure.

**2.2.6.** Supplier shall preserve the information pursuant to Section 2.2.1 to 2.2.5 for, at least, the duration of the Order.

**2.3. Compliance with Data Protection Laws.** Each Party shall comply with its obligations under Data Protection Laws. Supplier shall provide reasonable assistance to Alight (or a client of Alight) with meeting its obligations under Data Protection Laws in relation to the Processing of Personal Information, taking into account the nature of Supplier's Processing and the information available to Supplier.

**2.4. Data Subject Rights.** Supplier shall promptly notify Alight if it receives any request from a Data Subject asserting rights under Data Protection Laws with respect to their Personal Information. Supplier will not respond to any such request except on the instructions of Alight or as required by Data Protection Laws, in which case Supplier shall to the extent permitted by such Data Protection Laws inform Alight of such requirement prior to such response. Supplier will provide Alight with reasonable assistance in its efforts to fulfill its obligations to respond to such requests, including by providing access to or information about, deleting or modifying the relevant Personal Information, in each case, to the extent required under and in accordance with Data Protection Laws. If Supplier is unable to provide any such assistance for reasons permitted under Data Protection Laws, Supplier shall promptly notify Alight of such fact and shall provide such assistance promptly after the reasons for not doing so have expired.

**2.5. Return and Destruction.** Upon written request of Alight following termination or expiration of the Order, Supplier shall, and shall require its Subprocessors to, (a) return a complete copy of all Personal Information to Alight by secure file transfer in Supplier's customary format and (b) delete or render permanently anonymous all

other copies of Personal Information. Supplier shall comply with any such written request within five (5) business days (or less, if required by Data Protection Laws). Supplier and its Subprocessors may retain Personal Information as necessary to fulfill the Purpose and comply with applicable law, in which case the terms of this DPA shall continue to apply to such Personal Information for so long as it is retained.

**2.6. Recordkeeping.** Supplier shall keep accurate and up-to-date records regarding any Processing of Personal Information, including (a) records regarding access to and security of the Personal Information, the purposes and categories of Processing the Personal Information and its Subprocessors and (b) any other records as required by Data Protection Laws.

**2.7. Employees.** Personal Information shall only be accessed by Supplier's employees and other personnel who require such access to assist Supplier in connection with the Purpose. Unless otherwise restricted by applicable local laws, Supplier will subject all new employees to a comprehensive pre-employment background check in accordance with local laws and customs. Supplier will require that written agreements that include non-disclosure and confidentiality provisions are signed by all new employees prior to their work on behalf of Supplier in conduct of the Services. Supplier will periodically provide employees with comprehensive data security and privacy training, not less than once per year.

**2.8. Subprocessors.** Supplier shall not subcontract any of the Processing without the prior authorization of Alight (and in certain cases, without the prior authorization by Alight's client). Supplier's approved Subprocessors are listed in **Exhibit A (Subprocessors)**. Any additional Supplier Subprocessors are subject to the prior written approval of Alight. A request for additional Subprocessor(s) shall be submitted at least twenty (20) business days prior to the engagement of such Subprocessor(s). Supplier shall make available materials evidencing each Subprocessor's ability to provide the level of protection of Personal Information required by this DPA. Supplier shall remain responsible for the use, disclosure or other Processing of Personal Information by any of its Subprocessors to the same extent as if such use, disclosure or other Processing was by Supplier. Before any Subprocessor Processes Personal Information, Supplier will carry out adequate due diligence to determine that such Subprocessor is capable of providing the level of protection of Personal Information required by this DPA. The arrangement between Supplier and each Subprocessor will be governed by a written contract that contains requirements that are consistent and no less stringent than those that apply to Supplier under this DPA. Supplier represents that it maintains a vendor security program that assesses Subprocessors' compliance with such contracts. Upon Alight's written request, Supplier shall make Subprocessor data protection terms available to Alight (redacted, if necessary, to protect any confidential information).

**2.9. Data Protection Impact Assessment and Prior Consultation.** Supplier shall provide assistance to Alight with any data protection impact assessments, and any consultations with supervising authorities or other data privacy authorities.

**Section 3. Security Measures and Policies.** Supplier shall implement and maintain appropriate physical, technical, organizational and administrative measures reasonably designed to protect against the unauthorized destruction, loss, access to or alteration of Personal Information, including the security measures in **Exhibit B (Technical and Organizational Measures)** attached hereto and incorporated herein. The security measures implemented by Supplier to protect Personal Information shall be consistent with, and no less stringent than, what is required under Data Protection Laws and will ensure a level of security appropriate to the harm that might result from a Data Security Incident (defined below) and the nature of the data to be protected. Supplier shall implement and maintain written privacy and information security policies consistent with industry standards and this DPA.

#### **Section 4. Data Security Incident Notification and Response.**

**4.1.** Supplier shall notify Alight without undue delay and in accordance with the requirements of applicable Data Protection Laws of any confirmed or reasonably suspected breach of security by Supplier or any of its Subprocessors leading to the unlawful or unauthorized access, alteration, destruction, disclosure or loss of Personal Information (a "Data Security Incident").

**4.2.** In the event of a Data Security Incident, Supplier shall, without undue delay, (a) investigate the impact of such Data Security Incident, (b) identify the root cause of such Data Security Incident, (c) remedy the Data Security Incident and (d) prevent a reoccurrence of such Data Security Incident.

**4.3.** Supplier will provide Alight, without undue delay, information regarding the nature and consequences of the Data Security Incident, to the extent known by Supplier, including any such information necessary to allow Alight to notify relevant parties in accordance with Data Protection Laws. Supplier shall update Alight at regular intervals about new or updated information involved the Data Security Incident.

**Section 5. Audits.** Notwithstanding any provision of the Order or other agreements that may exist between the Parties to the contrary, Alight may, at its own expense and upon reasonable advance notice to Supplier, audit Supplier's books, records and other documents to the extent necessary to verify Supplier's compliance with the terms of this DPA; provided that Alight may not exercise its audit rights hereunder more than one time in any calendar year (unless required by a client of Alight, as a follow-up audit after discovery of a non-compliance issue or otherwise required by law or in connection with any audit initiated by a governmental entity having jurisdiction over Alight or a client of Alight). Each such audit shall occur during normal business hours and shall not unreasonably interfere with Supplier's normal business operations, and Supplier shall not be required to disclose or otherwise provide access to any information the disclosure of which would cause Supplier to violate any confidentiality obligation or applicable law. Alight may engage a third party to conduct any such audit so long as such third party is not a competitor of Supplier and enters into a confidentiality agreement. Audits under this DPA shall be subject to any additional terms and conditions regarding audits in the Order that do not conflict with the terms in this Section 5.

**Section 6. Details of Processing.** Certain information regarding Supplier's Processing of Personal Information required by Article 28(3) of GDPR is set forth in **Exhibit C (Details of Processing)** attached hereto and incorporated herein. Alight may make reasonable amendments to **Exhibit C** by notice to Supplier from time to time as Alight reasonably considers necessary to meet such requirements.

**Section 7. Restricted Transfers.** If the Parties anticipate a Restricted Transfer, Alight and Supplier hereby agree to enter into the SCCs with Alight as Data Exporter and Supplier as Data Importer (or as applicable). The SCCs shall come into effect on the commencement of the Restricted Transfer and shall reference and be incorporated into this DPA. In the event of any conflict or inconsistency between this DPA and the SCCs, to the extent of such conflict or inconsistency, the SCCs shall prevail. The Parties confirm that **Exhibit C** shall be deemed Annex 1 to the SCCs and that the security measures taken set forth in **Exhibit B** shall be deemed to be Annex 2 of the SCCs.

**Section 8. HIPAA.** If any "protected health information" (as defined under HIPAA) is created, received, maintained or transmitted by or on behalf of Supplier for Alight, then Supplier and Alight shall execute a HIPAA business associate agreement ("BAA"). If, in Alight's determination, such BAA is necessary, it shall be executed by the Parties, set forth in **Exhibit D (Business Associate Agreement)** and incorporated into this DPA. In the event of any conflict or inconsistency between this DPA and **Exhibit D**, to the extent of such conflict or inconsistency, Exhibit C shall prevail with respect to the matters therein.

**Section 9. Alight Affiliates & Clients.** The terms of this DPA shall apply equally to any Personal Information Processed by or on behalf of Supplier for any Alight affiliate or client. .

**Section 10. Term; Effect of Termination.** The term of this DPA shall begin on the Effective Date and shall continue for so long as the Order remains in effect or Supplier or any of its Subprocessors possesses or retains any Personal Information. The rights and obligations of the Parties which, by their nature, should survive termination or expiration of this DPA, shall survive such termination or expiration.

**Section 11. Miscellaneous.**

**11.1. Entire Agreement.** This DPA shall be deemed incorporated into and a part of, the SFA, but to the extent of any conflict or inconsistency between the DPA and the SFA, the DPA shall supersede the SFA for purposes

of this DPA. Except as expressly provided in this DPA, all of the terms and provisions of the SFA are and will remain in full force and effect and are hereby ratified and confirmed by the Parties. This DPA, together with the SFA, constitutes the sole and entire agreement of the Parties with respect to the subject matter hereof and thereof, and supersedes all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, with respect to such subject matter. For the avoidance of doubt, all claims and liabilities arising from or related to this DPA shall be brought under and subject to the terms of the SFA, including any provisions therein regarding indemnification, limitation of liability, dispute resolution, choice of law or choice of forum.

**11.2. Severability.** If any provision of this DPA, or the application thereof to any person, place or circumstance, shall be held by a court of competent jurisdiction to be invalid, void or unenforceable, the remainder of this DPA and such provision as applied to other persons, places or circumstances shall remain in full force and effect and such invalid, void or unenforceable provision shall be enforced to the fullest extent permitted by law.

**11.3. Amendment; Waiver.** The Parties agree to take such reasonable actions as are necessary to amend this DPA from time to time as is necessary for the Parties to comply with Data Protection Laws. This DPA may not be amended or otherwise modified unless such amendment or modification is set forth in writing, identified as amendment or modification of this DPA and signed by an authorized representative of each of the Parties. No provision of this DPA may be waived unless such waiver is set forth in writing, identified as a waiver of this DPA and signed by an authorized representative of the waiving Party. Except as otherwise provided in this DPA, no failure or delay by a Party in exercising any right under this DPA shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right.

**11.4. Assignment.** Neither Party may assign this DPA or any of its rights herein without the prior written consent of the non-assigning Party and any purported assignment without such consent shall be void and unenforceable; provided that each Party may, without obtaining such consent, assign this DPA as part of an assignment pursuant to and in accordance with the SFA.

**11.5. No Third Party Beneficiaries.** This DPA shall be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns and except with respect to Alight affiliates, nothing herein, express or implied, is intended to or shall confer upon any other person any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this DPA.

**11.6. Relationship of the Parties.** The relationship between the Parties is that of independent contractors and this DPA will not establish any agency, partnership, joint venture, fiduciary, franchise or employment relationship between the Parties (or between one Party and a representatives of the other Party). Neither Party by virtue of this DPA shall have any right, power or authority, express or implied, to bind the other Party.

**11.7. Force Majeure; Excused Performance.** Notwithstanding anything to the contrary in this DPA, Supplier shall not be liable for, nor be deemed to be in breach of this DPA as a result of, any failure to comply with its obligations hereunder or any other act or omission, to the extent such failure is directly attributable to (a) any failure by Alight to comply with its material obligations hereunder or under Data Protection Laws, (b) any act or omission of any vendor or other representative of Alight (other than Supplier and its Subprocessors) or (c) any act of God or other act or circumstance beyond the reasonable, unforeseeable, and unavoidable control of Supplier; provided that nothing in this Section shall limit or otherwise affect Supplier's obligation to execute its business continuity and disaster recovery program (which shall be in place and maintain during the entire duration of the Order). Each of the Parties shall use commercially reasonable efforts to mitigate the effects of any of the foregoing circumstances.

**11.8. Counterparts.** This DPA may be executed in any number of counterparts, each of which when so executed and delivered shall constitute an original, but such counterparts shall constitute one and the same instrument. This DPA may be executed and delivered electronically.

**11.9. Interpretation.** Any ambiguity in this DPA shall be resolved in favor of a meaning that permits both Parties to comply with Data Protection Laws. Unless the express context otherwise requires, the words "hereof",

“herein”, “hereunder” and words of similar import refer to this DPA as a whole and not to any particular provision of this DPA, references to a specific section refer to the sections in this DPA unless otherwise expressly provided and the words “include”, “including” and words of similar import shall be deemed to be followed by the words “without limitation”. The captions or headings in this DPA are for convenience only and shall not be considered a part of or affect the construction or interpretation of any provision of this DPA.

**11.10. Notices.** All notices under this DPA to Supplier shall be sent to le. All notices under this DPA to Alight shall be sent to [legalrequests@alight.com](mailto:legalrequests@alight.com).

**IN WITNESS WHEREOF**, the Parties have caused this DPA to be duly executed by its authorized representative, as of the Effective Date.

[ALIGHT CORPORATE NAME]

[~~SUPPLIER CORPORATE NAME~~ **MOURI TECH PRIVATE LIMITED**]

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

**Exhibit A – Subprocessors**

<b>Name of Subprocessor</b>	<b>Address of Subprocessor</b>	<b>Processing Operations of Subprocessor</b>	<b>Restricted Transfer (Yes/No)</b>



## Exhibit B – Technical and Organizational Measures

1. **Physical Security.** Supplier maintains security controls for entry points, holding areas, telecommunications areas and cabling areas that contain information processing systems or media containing Personal Information. Security controls include:
  - a. Access control and restriction by use of a defined security perimeter, appropriate security barriers, security cameras, entry controls and authentication controls, and maintenance of access logs for a period of time specified by law or policy. All system clocks must be synchronized with national or international time source;
  - b. Where Supplier ID cards are deployed, a requirement for all personnel, vendors, contractors and visitors to wear some form of visible identification to identify themselves as employees, contractors, vendors or visitors;
  - c. A clear desk/clear screen policy;
  - d. An automatic idle-lock for unattended equipment;
  - e. A requirement for visitors to Supplier's premises to be escorted at all times; and
  - f. Where technically feasible and commercially reasonable, cameras and CCTVs.
2. **Business Continuity and Disaster Recovery.** Supplier maintains the following business continuity controls and safeguards:
  - a. Business continuity and disaster recovery program is based on generally accepted industry practices designed to reduce the effects of a significant disruption in Supplier's operations;
  - b. Business continuity and disaster recovery programs are tested at least annually;
  - c. Backups of Supplier systems and software used in the delivery of Services are replicated to its disaster recovery facility so that recovery can take place when there is a disaster; and
  - d. Data is replicated to its disaster recovery facility, providing a scheduled point in time backup of the data to ensure integrity.
3. **Network Security Controls.** Supplier maintains the following network security controls and safeguards:
  - a. Defense-in-depth design with perimeter routers, network switches and firewall devices and default deny-all policy to protect internet presence;
  - b. Least privilege and authenticated access for network users and equipment;
  - c. Control of internet access by proxies;
  - d. Two-factor authentication for remote access with a non-reusable password;
  - e. Intrusion detection system to monitor and respond to potential intrusions;
  - f. Real-time network event logging and investigation using a security information event management tool;
  - g. Content filtering and website blocking using approved lists;
  - h. Limitations on wireless access to the network;
  - i. Policies and standards for wireless network devices;
  - j. Prohibitions on bridging of wireless and other networks, including the corporate network; and
  - k. Detection and disassociation of rogue wireless access points.
4. **Platform Security Controls.** Supplier maintains the following platform security controls and safeguards:
  - a. Maintenance of configuration/hardening standards;
  - b. Control of changes through an internal change control process;
  - c. Prohibition on installing unauthorized hardware and software;
  - d. Where technically feasible, automatic session timeouts after periods of inactivity;
  - e. Removal of vendor-supplied defaults (accounts, passwords and roles) during installation;

- f. Removal of services and devices that are not required by valid business needs;
  - g. Use of an anti-virus program with timely updates;
  - h. Non-privileged account access on workstations and laptops;
  - i. Full disk encryption and active firewall installation on laptops;
  - j. Development and test platforms will be segregated from operational platforms used in providing the Services;
  - k. Development tools such as compilers, assemblers, editors and other general-purpose utilities within the production environment will not be permitted unless expressly required for the delivery of the Services, in which case access is restricted; and
  - l. Software and hardware used in the delivery of the Services will be updated in line with industry standards, vendor support and security guidelines.
- 5. Application Security Controls.** Supplier maintains the following application security controls and safeguards:
- a. Defense-in-depth with the use of n-tier architecture for separation and protection of data;
  - b. A secure software development life cycle (SSDLC) for application development that includes training, development, testing and ongoing assessments;
  - c. Documentation, review, testing and approval before changes are implemented into production;
  - d. Identification, testing and remediation of application vulnerabilities and patches in a timely manner; and
  - e. A prohibition on using production data in development and testing environments.
- 6. Data and Asset Management.** Supplier maintains the following data and asset management security controls and safeguards:
- a. Technical, administrative and physical safeguards;
  - b. Regular backups and storage of Personal Information;
  - c. Encryption of Personal Information transmitted over public networks and on removable media;
  - d. Use of a data loss prevention tool for end point data transfer activities involving social security numbers or other national identification numbers;
  - e. Use of an inventory program to control the installation, ownership and movement of hardware, software and communications equipment;
  - f. Encryption, sanitization, destruction, or purging of all physical media containing Personal Information leaving Supplier's custody to ensure that residual magnetic, optical, electrical or other representation of data has been deleted, and is not recoverable; and
  - g. Logical separation of Personal Information of Alight and each of Alight's client's Personal Information from one another, and from the other clients of Supplier.
- 7. Access Control and Management.** Supplier maintains the following access control and management security controls and safeguards:
- a. Monitoring and logging access and use of the Supplier systems that contain Personal Information, including logging of access attempts to the Supplier systems that contain Personal Information with regular reviews of logs and necessary actions to protect against unauthorized access or misuse;
  - b. Periodic review and validation of role-based access to Personal Information and prompt removal of unnecessary access;
  - c. Unique logon ID and passwords;
  - d. Strong passwords with minimum length, complexity and expiration requirements;
  - e. Disabling access after a limited number of failed login attempts; and
  - f. Rejection of previously used passwords.

- 8. Risk Management.** Supplier maintains the following risk management controls and safeguards:
- a. An information security risk management system aligned to ISO 27001 standard (BS EN ISO/IEC 27001);
  - b. A cycle of risk assessments of critical assets, the frequency of which are dependent on the number of residual risks identified at each site;
  - c. Risk analysis is documented using standardized risk assessment templates; and
  - d. Risk management activities are established when risks are defined and agreed with the asset owners.
- 9. Vulnerability and Patch Management.** Supplier takes the following measures designed to identify and mitigate vulnerabilities that threaten Supplier's ability to enforce the confidentiality, integrity, and availability of Personal Information:
- a. A vulnerability monitoring process that provides alerts or notifications of new fixes available, and the resulting timeframe for remediation;
  - b. Regular scanning to identify and remediate vulnerabilities promptly;
  - c. Classification of vulnerabilities based on severity to allow for remediation based on predetermined service level expectations; and
  - d. Penetration tests at least once annually and prior to any new release or upgrade, on applicable Supplier environments, including perimeter vulnerability testing, internal infrastructure vulnerability testing and application testing.

## Exhibit C – Details of Processing

### Processing Operations

*The Processing operations to be carried out under this DPA are as follows:* The Personal Information received on behalf of Alight will be used for providing services, software under the Order (e.g., payroll and other business process outsourcing services, benefits-related services, software consulting and related activities) and may include, but are not limited to:

- providing data processing software, equipment, and services through various tools, applications and vendors;
- storing Personal Information;
- preventing unauthorized access to or modification of Personal Information (and other non-Personal Information);
- programing, printing and assembling, reviewing, and modifying statements as directed by Alight;
- communicating with data subjects in connection with services provided to Alight; and
- providing reference materials as requested by Alight.

The purpose of the processing operations above is to provide the Services in accordance with the Order.

### Data Subjects

*The Personal Information to be Processed by Supplier for or on behalf of Alight concern the following categories of data subjects:* current, former and/or prospective employees, their relatives and family members and other representatives of Alight, Alight's affiliates or clients of Alight.

### Categories of Personal Information to be Processed

*The Personal Information processed by Supplier comprise of the following categories:*

*HR/Employee data: that may include but is not limited to: full name; employee identification number; contact information (including home and work address, home and work telephone numbers, mobile telephone numbers, web address data, home and work email address); marital status; citizenship information; date of birth; gender; drivers' license information; national and governmental identification information; financial information (including salary and account balances); benefit program information (including benefit elections, beneficiary information, claims information, benefit plan account numbers and balances, and date of retirement); payroll information; professional or employment information (including date of hire, employment status, pay history, tax withholding information, performance records, leave information, and date of termination); and such other personal information that may be transferred from (or on behalf of) Alight to Supplier for performing services for Alight.*

*Related persons' data: may include but not limited to: name, date of birth, gender and contact information of dependents or beneficiaries (including home address; home and work telephone numbers; mobile telephone numbers).*

### Special categories of Personal Information

The Personal Information processed by Supplier may include sensitive personal data including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, health, genetic, biometrics or medical records, or/and criminal records.

## Exhibit D – Business Associate Agreement

### SUBCONTRACTOR BUSINESS ASSOCIATE AGREEMENT

This agreement ("**Business Associate Agreement**"), by and between Alight Solutions LLC ("**Alight**") and EPI - USE, Inc ("**Subcontractor**") (each individually, a "**Party**" and collectively, the "**Parties**") is effective as of January 7, 2022 (the "**Effective Date**").

**WHEREAS**, Company accesses, uses, transmits, or discloses protected health information ("**PHI**") to perform certain functions or activities on behalf of a covered entity or other business associates ("**Covered Entities**");

**WHEREAS**, Company subcontracts a portion of those services to Subcontractor pursuant to an agreement between Company and Subcontractor ("**Agreement**");

**WHEREAS**, in performing the services, Subcontractor may access, use, transmit or disclose PHI; and

**WHEREAS**, the Parties desire to comply with the Health Insurance Portability and Accountability Act of 1996, Pub. L. no. 104-191, the privacy standards adopted by the U.S. Department of Health and Human Services ("**HHS**") as they may be amended from time to time, 45 C.F.R. parts 160 and 164, subparts A and E (the "**Privacy Rule**"), the security standards adopted by HHS as they may be amended from time to time, 45 C.F.R. parts 160, 162 and 164 subparts C (the "**Security Rule**"), and the Privacy provisions (Subtitle D) of the Health Information Technology and for Economic Clinical Health Act, Division A, Title XIII of Pub. L. No. 111-5, and its implementing regulations (the "**HITECH Act**"). All such laws and regulations shall be collectively referred to herein as "**HIPAA**."

**NOW THEREFORE**, for and in consideration of the recitals above and the mutual covenants and conditions herein contained, Company and Subcontractor agree as follows:

1. **DEFINITIONS.** Capitalized terms used in this Agreement and not otherwise defined shall have the meanings set forth in HIPAA. The terms "use", "disclose" and "discovery", or derivations thereof, although not capitalized, shall also have the same meanings set forth in HIPAA and its implementing regulations.
  - (a) "**Breach**" shall have the same meaning as the term "breach" in 45 C.F.R. § 164.402.
  - (b) "**Electronic Protected Health Information**" or "**Electronic PHI**" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to the information that Company and Subcontractor create, receive, maintain or transmit from or on behalf of Covered Entities or Company.
  - (c) "**Individual**" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 502 (g).
  - (d) "**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Company and Subcontractor on behalf of Covered Entities.
  - (e) "**Required by Law**" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
  - (f) "**Secretary**" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.
  - (g) "**Unsecured PHI**" shall have the same meaning as the term "Unsecured Protected Health Information" in 45 C.F.R. § 164.402.
2. **OBLIGATIONS AND ACTIVITIES OF SUBCONTRACTOR.**
  - (a) **Permitted Uses and Disclosures.** Subcontractor shall use or disclose PHI only as permitted or required by this Business Associate Agreement, or as Required by Law.

- (b) **Minimum Necessary.** Subcontractor shall make reasonable efforts to limit requests for, and uses and disclosures of, PHI to a Limited Data Set (as defined in 45 C.F.R. § 164.514(e)(2)) or to the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request. Subcontractor shall comply with any regulations and guidance issued by the Secretary on what constitutes the minimum necessary for Subcontractor to perform its obligations under this Business Associate Agreement, the Agreement, or as Required by Law.
- (c) **Safeguards.** Subcontractor shall use appropriate physical, technical and administrative safeguards to prevent the unauthorized access, use or disclosure of PHI, including but not limited to Electronic PHI, other than as permitted or required by this Business Associate Agreement. Subcontractor also shall comply with Subpart C of 45 CFR Part 164 with respect to Electronic PHI.
- (d) **Security Incidents.** Subcontractor shall immediately report to Company any Security Incident of which Subcontractor becomes aware. Notwithstanding the foregoing, Subcontractor shall not be under any obligation to notify Company of Unsuccessful Security Incidents. "Unsuccessful Security Incidents" shall mean, pings and other broadcast attacks on Subcontractor's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.
- (e) **Breaches.** In the event of a Breach or suspected Breach, including any actual, successful Security Incident of which it becomes aware, Subcontractor shall send to Company within twenty-four (24) hours after such Breach or suspected Breach is discovered by Subcontractor, a written notice including, to the extent known: the names of the individuals whose information was breached, the circumstances surrounding the breach, the date of the breach and date of discovery, the information breached, the steps Subcontractor (or its agent or subcontractor) is taking to investigate the breach, mitigate losses, and protect against future breaches, and a contact person for more information
- (f) **Mitigation.** Subcontractor shall mitigate, to the greatest extent practicable, any harmful effect that is known to Subcontractor resulting from any successful Security Incident or Breach. Subcontractor agrees to cooperate with Company and shall provide such assistance as Company may reasonably request so that Company may comply with any obligations it may have to investigate, remediate, mitigate, report, notify or otherwise respond to a successful Security Incident or Breach. To the extent Company incurs any expenses that it reasonably determines to be necessary to mitigate any potential harm arising from a successful Security Incident or Breach by Subcontractor, its agents, or its subcontractors, Subcontractor shall reimburse Company for such expenses.
- (g) **Notices to Third Parties.** Subcontractor shall fully cooperate with Company and Covered Entities, as directed by Company, to make any notifications to Individuals, the Secretary, or the media. Subcontractor shall not make any notifications directly to Individuals, the Secretary, or the media without prior written approval from Company. Subcontractor shall be fully responsible for paying for all costs and expenses associated with making such notifications and for all costs and expenses related to remediation and mitigation of potential harm, including without limitation, reasonable legal fees Company or Covered Entities incur arising from any Breach of Unsecured PHI caused by Subcontractor, its agents, or its subcontractors and or any claims, demands, fines, judgments, actions or proceedings arising out of or in any way connected with the Subcontractor's performance under this Agreement. Subcontractor's obligations hereunder shall be in addition to, and in no way shall limit Subcontractor's indemnification obligations set forth in the Agreement.
- (h) **Agents.** Subcontractor shall ensure any agent or subcontractor to whom it provides PHI shall agree to restrictions and conditions that are the same or more stringent as those that apply through this Business Associate Agreement to Subcontractor.
- (i) **Access to Information.** To the extent that Subcontractor possesses or maintains PHI in a Designated Record Set, Subcontractor shall, within five (5) business days of receiving a request, provide Company with access to PHI about an Individual contained in a Designated record set in order for Covered Entities or Company to comply with the requirements under 45 C.F.R. § 164.524. In the event a request for

access to PHI by an Individual is made directly to Subcontractor, Subcontractor shall immediately forward the request to Company.

- (j) **Amendment of Protected Health Information.** To the extent that Subcontractor possess or maintains PHI in a Designated Record Set, Subcontractor shall, within five (5) business days of receiving a request, make available PHI for amendment and incorporate any amendments to PHI in a Designated Record Set that Covered Entities or Company directs or agrees to under 45 C.F.R. § 164.526. In the event a request for amendment to PHI by an Individual is made directly to Subcontractor, Subcontractor shall immediately forward the request to Company.
- (k) **Accounting of Disclosures.** Subcontractor shall document disclosures of PHI and information related to such disclosures as would be required for Covered Entities or Company to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Subcontractor shall provide to Company within five (5) business days of receiving a request, all information documented pursuant to this Section. In the event a request for an accounting of disclosures of PHI by an Individual is made directly to Subcontractor, Subcontractor shall immediately forward the request to Company.
- (l) **Encryption.** Subcontractor shall implement and maintain technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals in accordance with guidance issued by the Secretary. Such requirements apply without limitation to any and all PHI on computers, servers, portable and non-portable devices and any and all electronic communications that include PHI, such as e-mail. Subcontractor agrees that in no event may PHI be stored on any hardware including laptops, mobile devices, storage devices or the like, unless such PHI is secured and encrypted consistent with the terms of this Business Associate Agreement.
- (m) **Secretary.** Subcontractor shall make its internal practices, books, and records, including policies and procedures, and PHI, relating to the use and disclosure of PHI, available to Company and to the Secretary, in a time and manner mutually agreed to by the Parties or designated by the Secretary, for purposes of the Secretary determining Covered Entities' or Company's compliance with HIPAA. If Subcontractor directly receives the request from the Secretary, then Subcontractor agrees to notify Company of the request within five (5) business days.
- (n) **Marketing and Receiving Remuneration in Exchange for PHI Prohibited.** Subcontractor shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual. Subcontractor shall not engage in marketing activities or the sale of PHI, as defined in HIPAA without prior written consent of Company and individual written authorization, as required by Law.

### 3. PERMITTED USES AND DISCLOSURES BY SUBCONTRACTOR.

- (a) Subcontractor may use or disclose PHI as permitted or required by this Business Associate Agreement, the Agreement, as Required by Law, or as directed by the Covered Entities or Company, provided that such use or disclosure would not violate the Privacy Rule if done by Company or Covered Entities.
- (b) Subcontractor may use PHI for the proper management and administration of Subcontractor, to carry out the legal responsibilities of Subcontractor, or as required by Law.
- (c) Subcontractor may disclose PHI for the proper management and administration of Subcontractor or to carry out Subcontractor's legal responsibilities provided that such disclosures are (i) Required by Law, or (ii) Subcontractor obtains, in writing, prior to making any disclosure to a third party (a) reasonable assurances from such third party that the PHI will be held confidential as provided under this Business Associate Agreement and used or further disclosed only as required by law or for the purpose for which it was disclosed to such third party, and (b) an agreement from such third party to notify Subcontractor immediately of any breaches of the confidentiality of the PHI. Subcontractor shall immediately notify Company of any such notification received by Subcontractor from a third party.
- (d) Only as permitted by the Agreement, Subcontractor may use PHI to provide Data Aggregation services to Covered Entities, as applicable, or Company as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

#### 4. COMPANY OBLIGATIONS.

- (a) Company shall notify Subcontractor any limitation(s) in a notice of privacy practices in accordance with 45 C.F.R. 164.520, if and to the extent that such limitation may affect Subcontractor's use or disclosure of PHI.
- (b) Company shall notify Subcontractor of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Subcontractor's use or disclosure of PHI.
- (c) Company shall notify Subcontractor of any restriction to the use or disclosure of PHI that the Covered Entities have agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Subcontractor's use or disclosure of PHI.
- (d) Company shall not request that Subcontractor use or disclose PHI in any manner that would not be permissible under HIPAA.

#### 5. TERM AND TERMINATION

- (a) **Term.** This Business Associate Agreement shall commence upon the Effective Date and shall terminate when all of the PHI provided by Company to Subcontractor, or created or received by Subcontractor on behalf of Company, is returned or destroyed.
- (b) **Termination for Cause.** Upon Company's knowledge of a material breach by the Subcontractor, Company may either:
  - i. Notify the Subcontractor of the breach and provide the breaching party thirty (30) days from the date of notice to cure the breach, and if Subcontractor fails to cure the breach within such cure period, terminate this Business Associate Agreement and the Agreement by providing written notice to Subcontractor; or
  - ii. Immediately terminate this Business Associate Agreement and the Agreement if the Subcontractor has breached a material term of this Business Associate Agreement and cure is not possible, which determination is within Company's sole discretion.
- (c) **Effect of Termination.** Upon termination of this Business Associate Agreement, Subcontractor shall return or destroy all PHI received from Company, or created or received by Subcontractor on behalf of Company. This provision shall apply to PHI that is in the possession of agents or subcontractors of Subcontractor. Subcontractor shall retain no copies of PHI. Following the destruction of PHI, Subcontractor shall provide a certificate of destruction to Company. In the event that Subcontractor determines that returning or destroying the PHI is infeasible, Subcontractor shall provide a writing to Company explaining the conditions that make return or destruction infeasible. Upon Company's approval of such conditions, Subcontractor shall extend the protection of this Business Associate Agreement to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Subcontractor maintains such PHI.

#### 6. MISCELLANEOUS

- (a) **Regulatory References.** A reference in this Business Associate Agreement to a section of the Code of Federal Regulations, the Privacy Rule, the Security Rule or to another section of HIPAA means the section as may be amended from time to time.
- (b) **Amendment.** The Parties agree to take such reasonable actions as are necessary to amend this Business Associate Agreement from time to time as is necessary for Subcontractor and Company to comply with the requirements of HIPAA.
- (c) **Survival.** The respective rights and obligations of Subcontractor under Section 2(c)-(g), Section 5(c), this Section 6(c) and Section 6(d) of this Business Associate Agreement shall survive the termination of this Business Associate Agreement.



- (d) **Supersede and Replace.** This Business Associate Agreement supersedes and replaces any previous version of this agreement or any agreement between the parties concerning the subject matter of this agreement.
- (e) **Interpretation.** Any ambiguity in this Business Associate Agreement shall be resolved to permit Subcontractor and Company to comply with HIPAA.
- (f) **Counterparts.** This Business Associate Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which shall constitute one binding agreement.
- (g) **Severability.** In the event any provision of this Business Associate Agreement is rendered invalid or unenforceable under any new or existing law or regulation, or declared null and void by any court of competent jurisdiction, the remainder of the provisions of this Business Associate Agreement shall remain in full force and effect if it reasonable can be given effect.

**ALIGHT SOLUTIONS LLC**

**NTT DATA**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

## **SCHEDULE 2**

### **BUSINESS CONTINUITY REQUIREMENTS**

#### **1. DEFINITIONS.**

As used in these Business Continuity Requirements, capitalized terms shall have the meanings set forth below. Capitalized terms used but not defined in these Business Continuity Requirements shall have the meaning assigned to them in the Agreement.

“BCP” means Supplier’s business continuity and business resumption plan.

“Contact Center Operations” means Supplier’s essential customer service/contact center functions required to provide Services to Alight and/or any Alight client.

“Disaster” means any incident or event as result of which is that (a) Supplier is unable to perform the Services as required by the Agreement and/or any SOW and (b) the Services are not reasonably expected to be recoverable or remedied within the applicable RTOs (as hereinafter defined) without recourse to the BCP.

“RTO” means the recovery time objectives as set forth in Section 8 of this Schedule.

“RPO” means the recovery point objectives as set forth in Section 8 of this Schedule.

#### **2. BCP REQUIREMENTS.**

Supplier will implement a BC that will include the development, documentation, and implementation of a plan of action that will guide Supplier in the return of essential business operations, and eventually to a full business recovery, following a Disaster to ensure the ability of Supplier and Alight to fulfill obligations under the Agreement or any SOW.

The BCP will minimally include provisions for the following:

- Identification of the management and membership of the Disaster response and recovery teams;
- Identification and documentation of required recovery actions which must be addressed during the Disaster;

- Identification of the availability of required resources and response capabilities for the Disaster response and recovery teams;
- Identification and documentation of information and record requirements, protection, and recoverability status;
- Development and implementation processes for communicating, both internally and externally, following the loss of existing telecommunications and/or facility access including process for addressing media inquiries to limit potential risk exposure due to unofficial disclosure of information;
- Training of the Disaster response and recovery teams in the performance of their specific tasks; and
- Ensuring that all third party support arrangements involved in the provision of Services have adequate Disaster back-up and recovery plans.

### **3. DATA BACKUP/RECOVERY.**

Supplier will use data backup practices and technologies to support both operational and Disaster recovery. Supplier will maintain acceptable retention for data backups to ensure that acceptable RPOs can be achieved. Changed application data files and operational software will be backed up daily. A weekly full backup will be included in the backup scheme for all files required to deliver the Services.

### **4. DATA CENTER OPERATIONS.**

Supplier's data center will allow for rapid and comprehensive recovery for Supplier's systems and applications due to a Disaster. If Supplier backs up data through the use of media, the media containing the data will be sent off-site daily.

### **5. CONTACT CENTER OPERATIONS.**

A portion of the BCP will address the strategies, personnel procedures and resources that Supplier will use to respond to any long-term disruption to any Supplier Contact Center Operations required to deliver the Services to resume essential business operations within targeted recovery windows.

### **6. BCP TESTING.**

#### **6.1. Frequency of Testing.**

Supplier will periodically update and test and certify to Alight the operability of the BCP in conformance with the standards set forth in the BCP, but in no event less than once during every twelve (12) month period routinely. In each test, Supplier will simulate a Disaster and will verify that critical application-processing elements are available and the data is current. The tested applications shall support services that are representative of the Services.

#### **6.2. Reporting.**

Supplier will make available a summary report of the applicable results of the test to Alight within 30 business days after the completion of each BCP test under Section 6.1 of this Schedule. In the event the results reveal unreasonable risks as to the ability of Supplier to transition to performance under the BCP, Alight and Supplier will meet to discuss and agree upon a timeframe for retesting and correcting defects in the BCP and will agree to revise the BCP in a manner acceptable to Alight.

#### **6.3. Alight Participation.**

Upon Alight's request, Alight and Supplier will mutually agree on the level of Alight's participation in BCP testing. At a minimum, BCP will allow a representative of Alight to be present for the BCP testing. There will be no charge to Alight or to any Alight client for any BCP testing as defined in these Business Continuity Requirements.

### **7. RECOVERY.**

Supplier will implement the BCP upon its declaration of a Disaster with the objective of recovering critical functions within the RTOs and RPOs set forth below based on the nature of the Services being provided. For purposes of this Section 7, "recovery of critical functions" refers to the restoration of critical functions to a state where the content of such critical functions is accessible to Alight and/or Alight clients, which may require the use of a work-around or alternative service provided by Supplier. The recovery of critical functions does not require that the critical functions perform in strict accordance with the Service Levels in the Agreement and/or any SOW, but in any event the critical functions will be substantially usable and accessible to Alight and/or the applicable Alight client as necessary. Alight and Supplier will mutually agree on such critical functions and systems and applicable RTOs based on the applicable systems and hosting arrangements and their criticality.

## **8. RTOs.**

### **8.1. Supplier Hosted Supplier System.**

The following RTOs apply to Disasters that impact the systems used by Supplier in connection with its provision of the Services that are hosted and used by Supplier.

<b>Critical Functions/Systems</b>	<b>RTO</b>	<b>RPO</b>
Data Processing Services	24 hours	Completed transactions replicated or backed up at time of Disaster
Voice Response	24 hours	Services made available and/or completed transactions replicated or backed up at time of Disaster
Customer Service Reps	48 hours	Ability to answer telephone calls and access Services to assist callers
Client and Third Party Interfaces	24 hours	Reestablishment of facilities or alternative means established to enable exchange of information

### **8.2. Alight Hosted System Managed on Alight Premises.**

To the extent the Services involve Alight's hosting software on Alight systems at any Alight premises, and Supplier is managing the operation of such Alight software and/or systems, then Supplier will use commercially reasonable efforts to cooperate with Alight to support Alight's disaster recovery plan in the event of an Alight-declared disaster.

## **9. CONTACTS.**

Alight and Supplier will provide key contact names and contact details to each other to enable effective communication in the event that Supplier invokes the BCP in response to a Disaster. It is recognized that a Disaster may occur at any time and such emergency contact may be required at any time. Both Supplier and Alight will provide 24/7 emergency coverage by phone or pager. Both Alight and Supplier agree to inform the other within twenty (24) business hours in the event of change to the designated emergency contact or contact details.

## **10. GENERAL.**

If Supplier fails to reinstate all or a material portion of the Services in accordance with the BCP, notwithstanding anything in the Agreement or any SOW, Alight will have the right to perform or secure from a third party any portion of the Services not reinstated; and recover from Supplier the costs of cover in providing or securing from a third party any portion of the Services not reinstated, for up to 180 days after any Disaster. In the event Supplier is unable to reinstate the Services within 90 days after a Disaster, Alight may terminate the Agreement or any SOW under the Agreement for breach and without any penalty upon 30 days written notice to Supplier. In the event of a Disaster, Supplier will not increase any fees under the Agreement or any SOW.

## **SCHEDULE 3**

### **INSURANCE REQUIREMENTS**

At Supplier's sole expense, Supplier shall maintain, throughout the entire Term of the Order and including the provision of any post termination services or transition services, the following insurance with companies which are authorized to provide the applicable insurance and with an A.M. Best's rating of A-VII or better or a comparable rating from another rating agency. The insurance coverage and limits required to be maintained by Supplier shall be primary to insurance coverage, if any, maintained by Alight or its client. Supplier's insurance shall provide coverage for all employees of Supplier and all independent contractors working under the direction of Supplier. Limits are shown in USD, and if provided in another currency other than USD, the limits should be the equivalent of those shown in USD.

Worker's Compensation or other similar social insurance in accordance with the laws of the country, state or territory exercising jurisdiction over the employee with the minimum limits required by law.

Employer's Liability insurance, including coverage for occupational injury, illness and disease, with minimum limits:

Bodily Injury by Accident	<b>\$1,000,000</b> each accident
Bodily Injury by Disease	<b>\$1,000,000</b> each employee
Bodily Injury by Disease	<b>\$1,000,000</b> policy limit

Commercial General Liability/Public Liability insurance in an amount not less than \$1,000,000 combined single limit per occurrence and \$2,000,000 in the aggregate for bodily injury and property damage. Policy is to include coverage for liability arising from premises/operations, products/completed operations, personal and advertising injury, contractual liability and broad form property damage. Alight, its subsidiaries, affiliates, directors officers, employees and specified clients shall be additional insured(s) under Supplier's Commercial General Liability insurance.

Commercial Automobile Liability insurance in an amount not less than \$1,000,000 combined single limit per occurrence for bodily injury and property damage covering the use of all owned, non-owned, and hired automobiles. Alight, its subsidiaries, affiliates, directors officers, employees and specified clients shall be additional insured(s) under Supplier's Automobile Liability insurance

Excess Liability insurance with respect to the Employers Liability, Commercial General Liability/Public Liability and Commercial Automobile Liability policies described above, in an umbrella form and on an occurrence basis with limits of at least \$5,000,000 per occurrence.

Professional Liability Insurance (Errors & Omissions) insurance in an amount not less than \$10,000,000 per claim for damages arising from any acts, errors or omissions arising out of the rendering of or failure to render professional services as contracted under this Agreement. Claims-Made policies shall be renewed each year for a period of two (2) years after Supplier's completion of the services or shall have an extended reporting period of two (2) years. When renewed or replaced, the policy retroactive date must coincide with, or precede start of work on the services.

7. Network Security/Privacy Liability/Cyber Liability insurance in an amount not less than \$10,000,000 per claim including, but not limited to, coverage for privacy and network security liability, 1st and 3rd party liability, wrongful disclosure of data, wrongful disclosure of any business confidential information, personally identifiable information or any personal or protected health information as defined by HIPAA and HITECH Acts and including applicable law, breach of security, including unauthorized access to a computer system or database, extortion and extortion related threats, payments and interruption, downtime, identification theft, web hosting (if applicable), regulatory proceedings, Payment Card Industry Data Security Standards (PCI-DSS) fines, penalties and costs, notification costs, credit monitoring service. Claims-Made policies shall be renewed each year for a period of two (2) years after Supplier's completion of the services or shall have an extended reporting period of two (2) years. When renewed or replaced, the policy retroactive date must coincide with, or precede start of work on the services.

8. Commercial Crime insurance, including blanket coverage for employee dishonesty and computer fraud for loss or damage arising out of or in connection with any fraudulent or dishonest acts committed by the employees of Supplier, acting alone or in collusion with others, including the property and funds of others in their possession, care, custody or control, with a minimum limit per event of \$10,000,000. Coverage shall be endorsed to name Alight and specified clients of Alight as a joint loss payee under a joint loss payee endorsement.

9. All Risk Property insurance with a minimum limit of \$1,000,000 to cover risks of damage or loss to Alight property in Supplier's care, custody and control. Valuation is to include full replacement cost.

Where permitted by law, all policies described in 1 through 9 above shall contain a waiver of the insurer's right of subrogation against Alight, its subsidiaries, affiliates, officers, directors, employees and specified clients.

Supplier will be financially responsible for all deductibles or self-insurance retentions under such policies.

Supplier shall furnish Alight with certificates of insurance evidencing compliance with the requirements listed above before commencing the services. Supplier will give Alight thirty (30) days' notice prior to cancellation or material reduction of such insurance. Supplier will not permit any insurance requirements contained herein to lapse. If Supplier cancels any insurance policy, Supplier will promptly replace such insurance policy without lapse in coverage. Supplier will ensure that any subcontractors will maintain insurance coverage as specified herein. Failure of Supplier to provide and maintain the insurance described herein will constitute a material default for which Alight will be entitled exercise all rights and remedies hereunder and those available under applicable law.

The insurance coverage and limits required above are minimum requirements and in no way limit the liability of Supplier, its employees, agents or subcontractors for their respective acts or omissions.

## **Schedule 4**

### **Alight's Supplier Code of Conduct**

#### **Introduction and Scope**

Alight is committed to the highest standards of ethical conduct, integrity, and corporate social responsibility. All suppliers to Alight are expected to conduct their business in accordance with the highest standards of ethical behavior and in accordance with applicable laws and regulations and Alight's policies on corporate conduct ("Supplier Code"). This Supplier Code applies to all suppliers and each of their vendors, suppliers, subcontractors and agents providing goods, software, or services directly or indirectly to Alight (each a "Supplier").

#### **Policy Compliance**

Alight may assess Supplier's compliance with this Supplier Code, and any violations of this Supplier Code may jeopardize the Supplier's business relationship with Alight, up to and including termination.

#### **Reporting and the Alight Ethics Helpline**

Alight *Code of Conduct* outlines the ethical standard for Alight employees, officers and directors, contractors, and suppliers as appropriate, and any agents, affiliates, partners or third parties representing Alight. Suppliers

are expected to report any suspected wrongdoing. The [Alight Ethics Helpline](#) or 1- 844-570-4239 is a convenient and anonymous way for Suppliers to report suspected wrongdoing without fear of retaliation. It is available 24 hours a day, 365 days a year. Alternatively, Appropriate action is taken against those found to have violated applicable law or Alight policy.

## **Treat people right**

Alight believes that all workers within our service delivery and supply chain deserve a fair and ethical workplace. Suppliers shall uphold these standards:

### **Harassment and discrimination**

Suppliers must promote a workplace that is free of discrimination in hiring and other employment practices, and not discriminate based on any protected status or characteristic. Suppliers will provide a work environment free from any form of harassment or discrimination of any kind, including behavior that is disrespectful, abusive or humiliating on the basis of gender, race, ethnicity, religion, sexual orientation, gender identity, national origin, age, disability, pregnancy, veteran status, marital or domestic partner status or any other status protected by law.

### **Diversity and equal treatment**

Alight believes that including diverse partners in our business is important to our success. We expect our suppliers to identify, adopt, and integrate diversity into their own supply processes and hiring, including equal treatment of minority and women-owned businesses in the supplier selection process.

Supplier shall provide equal treatment without regard to any protected status or characteristic in all aspects of Supplier's employment decisions, including:

- Recruitment and hiring
- Promotion and performance
- Development and training
- Benefits and compensation
- Termination of employment

### **Maintaining a safe and healthy workplace**

Suppliers shall provide workers with a safe and healthy workplace that complies with all applicable health and safety laws and regulations. Suppliers must take proactive measures to prevent workplace hazards. This commitment to safety also means that Suppliers must never tolerate any threats or acts of violence, including intimidation, bullying, and attempts to instill fear in others.

### **Human rights and labor concerns**

#### **No forced or child labor**

Suppliers shall not engage in or permit forced labor, human trafficking or underage labor. Additionally, Supplier must not employ or allow employees under 15 years old or the legally required minimum age, whichever is higher.

#### **Wages**

Suppliers shall provide wages and benefits that met or exceed local legal requirements and provide them in a timely manner.

#### **Freedom of association and collective bargaining**

Supplier shall respect the rights of its workers to freely choose whether or not to join associations, organizations and trade unions, and to bargain collectively as provided by local law or regulation.

## **Follow the laws and our policies**

Compliance means not only observing the law, but also conducting corporate business in a way that recognizes and fulfills social and ethical responsibilities. In addition to any specific obligations under the Supplier's agreement with Alight, Supplier shall adhere to the following standards:

### **Anti-bribery and anti-corruption laws**

Alight is committed to compliance with anti-corruption laws in all countries where Alight operates and expects the same of its Suppliers. These laws include the U.S. Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act, U.S. fraud statutes, state laws and similar international rules. The laws prohibit improper payments, such as bribes and kickbacks, or promises to make improper payments, whether or not the offer is successful. The offering, paying, soliciting or accepting of bribes or kickbacks is strictly prohibited. Supplier shall not make or promise to make an illegal payment or otherwise offer anything of value to any government officials or anyone else for the purpose of securing an improper advantage or to obtain or retain business.

### **Fair dealing and marketing practices**

Alight competes fairly in the marketplace and abides by fair competition and antitrust laws and expects the same of its Suppliers. Supplier shall not enter into any agreements, whether express or implied, that violate the letter or spirit of anti-competition laws. In addition, Supplier shall not alter or draft agreements with Alight to conceal or falsify deal terms. We expect Supplier's marketing and sales activities on Alight's behalf to be ethical.

### **Financial crime, anti-money laundering and anti-terrorism laws**

Supplier shall comply with the financial crime, anti-money laundering and anti-terrorism laws in all jurisdictions where it does business. Alight will conduct business only with reputable parties that are engaged in legitimate business activities with funds derived from legitimate sources. Supplier will not accept funds known to be derived from illegal activities.

### **International trade restrictions**

Supplier shall comply with U.S. trade restriction laws and regulations, including economic sanctions, applicable import/export rules and anti-boycott activities and expects the same of its Suppliers. These import and export laws apply not only to goods but also to technology, software, intellectual property and technical information. Complying with all applicable international trade restriction and economic sanctions laws includes never knowingly employing or doing business with anyone suspected of being connected with criminal or terrorist activities or who is subject to economic sanctions.

### **Accepting and giving gifts and entertainment**

Supplier shall ensure that acceptance of any business courtesies, gifts, or entertainment by any of its personnel is proper and consistent with the Anti-Corruption rules. Supplier shall not offer gifts or entertainment to Alight employees at any time during a Request for Proposal (RFPs) or other supplier-selection process.

### **Avoid conflicts**

At Alight, we act with integrity and avoid conflicts that may prevent us from acting in the best interest of our clients and expect the same from our Supplier. Supplier shall disclose actual or potential conflicts of interest relating to their activities with Alight.

### **Environmental Responsibility**

Alight is committed to providing service in a manner that maintains a safe and healthy workplace for our Colleagues and minimizes our potential impact on the environment. Supplier will operate a safe and healthy workplace in an environmentally responsible and efficient manner to minimize adverse impacts on the environment. Supplier will abide by Alight's environmental policy communicated to Supplier from time to time, and will upon request, provide Alight with details regarding its compliance with Alight environmental policy, and the percentage of Suppliers' operations covered by ISO 14001 (Environmental Management System).



## **Protect Alight and data in our care**

Subject to the terms of any specific contractual provisions that apply, Supplier shall comply with all laws and regulations regarding the security and privacy of information (including personal data, personally identifiable information and personal health information), data protection and cross-border data transfers. In addition, Supplier shall maintain appropriate documents and records to ensure regulatory compliance.

## **Training**

Supplier shall maintain a training program adequate to ensure that management and employees comply with all regulatory requirements and expectations set forth in this Supplier Code. Supplier shall cooperate with Alight as needed to develop and maintain employee training programs to implement the policies and topics outlined in this Supplier Code. Supplier shall ensure that its personnel read and comply with the Supplier Code and all associated training. Depending on the nature of the goods or services, Alight may require Supplier's personnel to certify compliance with Alight's Supplier Code. Training topics may include:

- Anti-Sexual Harassment;
- Anti-Corruption;
- Data Privacy including HIPAA and GDPR (where applicable);
- Data Security; and
- Diversity

Alight may require training on additional topics depending on the services to be provided and applicable jurisdictions and laws. Upon reasonable request, Supplier shall provide Alight with evidence of training assignment and completion.

## **Schedule 5**

### **Background Checks Requirements**

#### **Summary**

Alight is committed to completing a comprehensive pre-employment background check on every new hire in North America, Asia-Pacific (APAC) and Europe, Middle East and Africa (EMEA) regions, and aspires to do so globally, in accordance with local laws and customs. Alight requires that Supplier follow a similar process to the extent permitted under applicable law.

#### **Standards for Locations Globally**

The types of background checks conducted globally will vary based on the laws and customs of the applicable countries, as well as available infrastructure for conducting background checks. Alight, however, has a global standard that strives to meet in all locations to the extent permissible, including:

- Verification of educational credentials, employment history, and criminal history.
- Where applicable, use of national ID numbers to conduct the review.
- A consistent means of validating eligibility across locations (e.g. falsification of educational credentials is a disqualifying result in all locations, within local legal limits).

**Employee Notification Requirement**

Supplier will ensure, to the extent permitted under applicable law, that it has a process in place where employees are required to report any criminal conviction after the completion of the background check to Supplier. To the extent that the conviction would have precluded Supplier from hiring the employee, Supplier will ensure that such employee is not engaged in the provision of services, products or software to Alight.

(continued on next page)

**Standard Country Checks**

<b>US</b> Education Report Employment Report (7 years) Criminal History (10 Years) Government Watch/Global Sanctions and Enforcement check Credit check (where required for role and Not Puerto Rico) SSN Trace  Widescreen Plus National Criminal Search
<b>Canada</b> Education Report Employment Report (7 years) Credit check (where required for role) Global Criminal Search (Government Source or Media Source) Global Sanctions and Enforcement
<b>UK</b> Global Education Global Employment (5 years) Global Criminal Search Global Credit Search Conduct Search Global Sanctions & Enforcement
<b>India</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Address Verification Global ID Check Global Sanctions and Enforcement check
<b>Poland</b> Global Education Global Employment (5 years) Global Sanctions & Enforcement
<b>Ireland</b> Global Education Global Employment (5 years) Global Criminal Search Global Credit Search Conduct Search Global Sanctions & Enforcement
<b>Australia</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Passport Verification Global ID Check

Global Sanctions and Enforcement check
<b>Singapore</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Passport Verification Global ID Check Global Sanctions and Enforcement check
<b>Hong Kong</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Address Verification Passport Verification Civil Litigation Global Credit History Check Professional Reference Check Report Global Sanctions and Enforcement check
<b>Thailand</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Global ID Check Global Sanctions and Enforcement check
<b>Malaysia</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Global ID Check Global Sanctions and Enforcement check
<b>Indonesia</b> Education Report Employment Report (5 years) Global Criminal Search (7 years) Address Verification Global ID Check Global Sanctions and Enforcement check

