Service Level Agreement (SLA) Template

Service Agreement

This agreement is made on [.] day of [.] 2022 [“Effective Date”]

Between

(1) **Company A** a company incorporated in the United Arab Emirates with its principal place of business in India at P.O. Box 5209, hereinafter referred to as ‘**COMPANY A**’ (which expression shall whenever the context permits be deemed to mean and indicate its successors in interest and assigns); and

(2) **[.]**, a company incorporated under the laws of the United Arab Emirates and registered with the Government of Dubai Department of Economic Development under the Commercial License Number [.]; having a principal place of business at [.] , hereinafter referred to as “**Service Provider**” (which expression shall whenever the context permits be deemed to mean and indicate its successors in interest and assigns).

Each a “Party” and together the “Parties"

Whereas

(A) The Service Provider represents to have the know-how, qualification and necessary ability and expertise to provide services to customers of organisations the size and type of COMPANY A.

(B) COMPANY A, wishes to obtain Services (as defined below) from the Service Provider as its independent non-exclusive external service provider on the terms of this Agreement, which the Service Provider has agreed on.

Now therefore, for good and valuable consideration receipt of which is hereby acknowledged, the Parties agree as follows:

1 Definitions and Interpretation

1.1 In this Agreement the following definitions shall apply.

Agreement means this agreement together with any variations, amendments or addendums to this agreement as may from time to time be agreed in writing by the Parties

Business Day means the working time in between 8a.m. to 5:p.m. from Monday to Friday (both days inclusive [excluding any public holidays] during which COMPANY A head office shall be open for routine business

Confidential Information means all confidential information (howsoever recorded, preserved or disclosed) disclosed by either Party to the other Party in connection with this Agreement whether before or on or after the Effective Date including:

a) business strategies, business arrangements, computer and network operations, functions and systems architecture; or
b) any technical, financial or commercial information; or
c) any information relating to COMPANY A or COMPANY A customers; or
d) any information that would be regarded as confidential by a reasonable business person; or
e) any information developed by the Parties in the course of carrying out this Agreement;
f) the existence and contents of this Agreement;

but not including any information that:

a) is or becomes generally available to the public other than as a result of its disclosure by the Receiving Party or its representatives in breach of this Agreement or of any other undertaking of confidentiality addressed to the Party to whom the information relates

(except that any compilation of public information in a form not publicly known shall nevertheless be treated as Confidential Information); or

b) the Parties agree in writing is not Confidential Information or may be disclosed; or
c) was available to the Receiving Party on a non-confidential basis prior to the disclosure by the Disclosing Party;
d) is developed independently by the Receiving Party without reference to the Confidential Information provided by the Disclosing Party;
e) is received from a third party which is under no obligation to maintain confidentiality
f) is required to be disclosed by law or regulatory requirement

Disclosing Party means a Party to this Agreement which discloses directly or indirectly Confidential Information to the Receiving Party;

Receiving Party means a Party to this Agreement that receives Confidential Information directly or indirectly from a Disclosing Party

Service Fees means the amounts payable for the Services (or any part thereof) calculated in accordance with schedule 2 (Service Fees).

Services shall have the meaning as detailed under clause 3.1

1.2 Any amendments/addendum to this Agreement shall form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Addendum.

1.3 Words in the singular shall include the plural and vice versa; a reference to one gender shall include a reference to the other genders; a reference to any "Party" shall include that Party's personal representatives, successors or permitted assigns.

1.4 The headings contained in this Agreement are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this Agreement

2 Term

2.1 This Agreement shall come into force on the Effective Date and shall continue in force for a period of one (1) Gregorian calendar year from the Effective Date (the "**Term**") unless earlier terminated in accordance with clause 15 of this Agreement.

3 The Services

3.1 The Service Provider shall provide required services which shall include but not limited to:

(a) The services as more detailed under Schedule 1;
(b) all, and/or (as the context requires) any obligations of the Service Provider under this Agreement,
(c) any services, functions and responsibilities (including any incidental service, functions or responsibility) that, whilst not specified in the Agreement as in scope, are reasonably required for or related to the proper performance and provision of the services; and
(d) any amendments to services, functions and responsibilities included in any of the above that are agreed between COMPANY A and the Service Provider to perform the Services in accordance with this Agreement.

all above together referred to as the ' **Services**'

3.2 Any acceptance or approval communicated by COMPANY A relating to the delivery or performance of the Services or any delay or omission to communicate such approval or

acceptance shall not relieve the Service Provider of its obligations to perform in accordance with this Agreement.

3.3 Nothing in this Agreement shall have the effect of preventing COMPANY A or any member of COMPANY A from providing, or appointing any third party to provide on its behalf and/or receive any services the same as or similar to the Services.

3.4 While providing the Services, the Service Provider shall:

(a) use its best endeavours to provide required Services and to represent the interests of COMPANY A in good faith;

(b) at all times act in compliance with the provisions of this Agreement and any instructions or guidelines notified by COMPANY A to the Service Provider from time to time;

(c) perform its duties and obligations under this Agreement with all due care, skill and diligence;

(d) at all times act in compliance with all applicable laws or regulations governing the Services;

(e) provide the Services in a way which enables the members of COMPANY A at all times to comply with all applicable relevant laws; and

(f) obtain and at all times maintain such licences, authorisations, exemptions and/or registrations to be held by it or any of its representatives under any applicable laws or regulations necessary for the purposes of the performance by it of any duties and obligations hereunder, and provide evidence of the same to the reasonable satisfaction of COMPANY A upon COMPANY A's request

(g) notify COMPANY A immediately on becoming aware of any breach or suspected breach by the Service Provider of any relevant laws, provide members of COMPANY A with such assistance as they may require to investigate such allegations and correct any breach, and on COMPANY A's request, do all such things as are necessary at its own cost in order to minimise the impact of such breach.

(h) not use and/or display any of COMPANY A’s intellectual property unless permitted by COMPANY A and in such event, use and/or display such intellectual property in such manner as may be approved by COMPANY A from time to time;

(i) submit all such reports, statements, information or documents as may be required by the provisions of this Agreement in the format and timeframes specified in this Agreement;

4 Service Levels

4.1 The Service Provider shall at all times use best endeavours to achieve or exceed the mutually agreed Service levels.

5 Service Fees and payment

5.1 In consideration of the performance of the Services, COMPANY A shall pay the Service Provider the Service Fees as set out in and/or as calculated in accordance with schedule 2 (Service Fees), which shall be invCompany Aed at the times and in the manner specified in this clause.

5.2 Unless otherwise expressly agreed between the Parties, the Service Fees payable by COMPANY A under this Agreement shall constitute COMPANY A's entire liability to the Service Provider under this Agreement.

5.3 Unless expressly agreed otherwise between the Parties:

(a) the Fees shall be payable by COMPANY A in United Arab Emirates Dirhams ('AED');
(b) invCompany Aes shall be submitted by the Service Provider in arrears on the [25th day] of each month and shall be payable by COMPANY A within 30 Business Days of the end of the month following the date of receipt of the relevant invCompany Ae by COMPANY A; and
(c) the Service Provider shall make available to COMPANY A, on a real-time basis and in a format readily accessible by COMPANY A, electronic records of all invCompany Aes relating to this Agreement, together with monthly statements of invCompany Aes paid and outstanding.

5.4 If COMPANY A receives an invCompany Ae from the Service Provider which it disputes in good faith, COMPANY A shall notify the Service Provider in writing of such dispute as soon as reasonably practicable and COMPANY A may withhold payment of such sums as are the subject of the dispute pending resolution of such dispute.

5.5 If the Service Provider commits a service level default or breach of this Agreement, COMPANY A shall have the right to suspend payment of such of the Service Fees as it considers (acting reasonably) are allocable to the Services which relate to the default (the 'Relevant Charges'), until the Default has been remedied, after which payment of the Relevant Charges so suspended shall (subject to any other rights of COMPANY A to suspend or withhold payment) be payable to the Service Provider.

5.6 Any overpayments by COMPANY A shall be a sum of money recoverable from the Service Provider.

5.7 Whenever under this Agreement which COMPANY A and the Service Provider are a party, a sum of money is recoverable from or payable by the Service Provider the same may be recovered or deducted from any sum due (or which at any time thereafter may become due) to the Service Provider under this Agreement.

6 Policies and Procedures

6.1 The Service Provider shall comply with all COMPANY A policies, timelines and instructions as advised by COMPANY A from time to time (including but not limited to those relating to security and health and safety).

7 Staff

7.1 The Service Provider shall ensure that its staff are suitably experienced, qualified, skilled and trained to the highest level expected of a specialist professional providing services similar to the Services to customers of the same nature as COMPANY A and shall ensure that such staff shall act at all times in a professional manner. The Service Provider shall at all times ensure that it complies with any requirements for any work permits, visas, rights of residence or other similar provisions in respect of its staff.

7.2 Nothing in the provisions of this Agreement creates or constitutes an employer-employee relationship between COMPANY A and the Service Provider or the Service Provider's staff.

The Service Provider acknowledges that the Service Provider is the employer and sponsor of the Service Provider's staff in accordance with the UAE Laws and regulations.

8 Assignment

8.1 This Agreement (and/or any document entered into pursuant to or in connection with it) may be assigned or transferred by COMPANY A, in whole or in part, at any time and on more than one occasion to one or more members of COMPANY A without the consent of the Service Provider.

8.2 The Service Provider shall not assign, transfer or otherwise deal with any right or obligation arising under or in connection with this Agreement (and/or any other document entered into pursuant to or in connection with it) except with the express prior written consent of COMPANY A which COMPANY A may grant or withhold in its absolute discretion.

9 The Service Provider's Representations and Warranties

9.1 The Service Provider represents and warrants to COMPANY A that:

(a) it is duly incorporated and is in good standing under the laws of the jurisdiction in which it is incorporated;
(b) it has the full power and authority to enter into and perform its obligations under this Agreement;
(c) it is suitably authorised by the applicable regulatory authorities to carry out the Services described in this Agreement;
(d) it has taken all necessary actions to authorise the execution, delivery and performance of this Agreement;
(e) this Agreement constitutes legal, valid and binding obligations, and is enforceable in accordance with its terms

10 COMPANY A's Representations and Warranties

10.1 COMPANY A represents and warrants to the Service Provider that:

(a) it is duly incorporated and is in good standing under the laws of the jurisdiction in which it is incorporated;
(b) it has taken all necessary actions to authorise the execution, delivery and performance of this Agreement;
(c) this Agreement constitutes legal, valid and binding obligations, and is enforceable in accordance with its terms; and
(d) it operates and conducts and will continue to operate and conduct its business in accordance with the requirements of all applicable laws.

11 Confidentiality

11.1 The Receiving Party shall not at any time without the prior written consent of the Disclosing Party:

(a) Utilise, copy employ or use in any manner any of the Confidential Information otherwise than in furtherance of its obligations under this Agreement;
(b) Disclose any of the Confidential Information to any third party, other than to any of the Receiving Party's representatives who are reasonably required in the course of their duties to receive and acquire the same and who are made aware of the confidentiality provisions contained in this Agreement. The Receiving Party shall be primarily liable for any breach of these provisions by any of its Representatives; and

(c) Make any copies of the Confidential Information or reproduce it in any form except for the purpose of supplying the same to those whom disclosure is permitted in accordance with this Agreement.

11.2 . The Receiving Party shall maintain Confidential Information in confidence and shall exercise in relation thereto no lesser security measures and degree of care than those which the Receiving Party applies to its own Confidential Information which the Receiving Party warrants as providing adequate protection against unauthorized disclosure, copying or use. Without affecting the generality of this obligation the Receiving Party shall keep all Confidential Information and all information generated by the Receiving Party based thereon as confidential and in such a manner that it would not allow any person not authorized to do so to have access to the Confidential Information.

11.3 The Parties shall ensure that disclosure of such Confidential Information is restricted to those of its employees, directors, professional advisers, consultants, reinsurers, brokers and/or representatives having the need to know the same for and/or related to and/or furthering the purpose of the Agreement.

11.4 Copies or reproductions shall not be made except to the extent reasonably necessary for the Permitted Purpose and all copies made shall also be subject to the confidentiality obligations and shall be the property of the Disclosing Party

11.5 The Receiving Party shall inform immediately (and in any case within 24hrs) to the Disclosing Party in case of becoming aware of or suspicion of any Confidential Information being disclosed to an unauthorised person or having been accessed in an unauthorized manner.

11.6 A Party may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction provided that, to the extent it is legally permitted to do so, it gives the other Party as much notice of such disclosure as possible.

11.7 Where either Party so requests and in any event at the end of the Term, the other Party shall without delay:

(a) return to the Disclosing Party, in a form capable of delivery, anything containing or recording the Disclosing Party's Confidential Information, whether in the form of documents, computer records, audio tapes, video tapes, CD ROMs or any other media; and

(b) certify in writing that any the Disclosing Party's Confidential Information not returned has been destroyed or made permanently unusable,

Except where the Party may be required to maintain one (1) copy of Confidential Information to meet its regulatory record keeping requirements and/or where it may not be practical to erase all electronic records/permanently archived records, provided the confidentiality obligations shall continue to apply for an indefinite period for all such records which are not destroyed

11.8 The Service Provider shall not whether before or after termination of this Agreement, use any of COMPANY A customer's information or any extract or part thereof directly or indirectly to solicit business from or to offer any or supply any products and / or services.

11.9 Wherever the Services relate to and/or wherever the Service Provider has access to any personal identifiable information ("PII") or personal health information ("PHI") of any of

COMPANY A or COMPANY A's customers/insured then the following provisions shall additionally apply:

(A) the Service Provider agrees:

(a) To apply best market security practices including enhanced security controls and restrictions to preserve confidentiality of all PHI or PII information as received from COMPANY A.

(b) Not to transfer, nor process, nor store any PHI or PII outside UAE. The Service Provider undertakes to always keep PHI and PII as received or accessed by the Service Provider within UAE at all times.

(c) Not to use any COMPANY A or COMPANY A customer related data/information (including PHI and/or PII) for any purposes other than as authorised by COMPANY A.

(d) Not to subcontract/assign to any third party without seeking prior written consent of Company A, provided always that the Service Provider prior to sending any COMPANY A data to any authorised third party must ensure that it has signed a detailed non-disclosure agreement to fully protect Confidential Information as received under this Agreement.

(e) Notwithstanding anything contrary mentioned in this Agreement, COMPANY A shall be and continue to be the owner of all PHI and PII data/information.

(f) COMPANY A retains the right to audit and/or monitor all activities of the Service Provider which involves any PHI or PII data/information.

(g) That upon termination or expiry of the Agreement, the Service Provider will permanently purge all PHI and PII information as much as may practically be possible. Wherever the Service Provider is unable to permanently destroy or needs to retain a copy of any PHI or PII data for its regulatory record keeping regulations then the Service Provider clearly acknowledges and agrees that all confidential obligations under this Agreement shall continue to apply on all such data/records (including PHI and PII data) retained by the Service Provider,

(B)The Service Provider represents and warrants that it conducts background verification checks on all candidates for employment, contractors, and third parties and as part of the same the Service Provider shall define background verification process addressing required regulatory/government requirements and has in place established criteria for verification checks based on (a) role of individual (b) classification of information access needed (c) access to critical areas (d) risks identified (e) as per any other regulatory/legal requirement

The Service Provider undertakes to fully comply with all COMPANY A Information Security policies and practices as and when communicated by COMPANY A

12 Intellectual Property Rights

12.1 Except as stated under clause 12.3, this Agreement shall not operate to assign any title, interest or intellectual property rights in any document, report, material and/or content, ideas provided by either Party to the other Party.

12.2 All title, interest and intellectual property rights in any content, idea or material whether created, modified or derived from that material shall belong to and vest with the same Party which originally owns the intellectual property of that material.

12.3 The Service Provider hereby assigns absolutely (and shall procure that all staff assigns absolutely) to COMPANY A or (at COMPANY A's option) any member of COMPANY A, by way of present assignment of existing and all future property, rights, title and interest, any and all intellectual property rights in any new material, report, data, intellectual property created pursuant to this Agreement all of which shall vest in COMPANY A immediately upon creation of the same with full title guarantee and free from all encumbrances, together with the right to take action for any past, present and future damages and other remedies in respect of any infringement or alleged infringement of such intellectual property rights.

13 Indemnities

13.1 The Service Provider shall indemnify, defend and hold harmless COMPANY A and each of its member (and their respective successors and assigns) in respect of any and all claims, losses, expenses, liabilities incurred or suffered by or made against any of them and whether wholly or in part resulting directly or indirectly arising from or connected with any of the matters including those listed below, whether or not such claims, losses, expenses and/or liabilities were foreseeable at the date of entering this Agreement:

(a) any claim that any Services provided by the Service Provider, or the use, reproduction or exploitation of any of the same by or on behalf any member of COMPANY A in accordance with this Agreement infringes a third party's intellectual property rights or rights in respect of any third party confidential information;

(b) any breach by the Service Provider of its obligations under this Agreement in relation to COMPANY A’s confidential information;

(c) the gross negligence; wilful misconduct or wilful default of the Service Provider;

(d) any fraudulent or dishonest act or omission by any member of the Service Provider;

(e) any claim relating to death or personal injury arising from the acts or omissions of any member of the Service Provider;

(f) any claim brought by a third party (including any COMPANY A’s client), to the extent that such claim is, or is alleged to be, caused by or contributed to or based on any act or omission of a member of the Service Provider;

(g) any fines levied on any member of COMPANY A by a third party including any relevant regulator arising from the acts or omissions of any member of the Service Provider;

(h) the breach by any member of the Service Provider of any relevant laws, or any obligations of the Service Provider under this Agreement which cause or contribute to any breach of any relevant laws by any member of COMPANY A;

(i) loss of or damage to any COMPANY A data, records, premises including costs and expenses associated with its recovery and/or reconstruction, to the extent that such loss is caused by or contributed to by any act or omission of any member of the Service Provider,

(j) any claim made by Service Provider’s staff in connection to any matter;

(k) the Service Provider not maintaining required licenses, authorisations, exemptions and/or registrations

(l) Any liability, loss, damage, injury, cost or expense incurred by COMPANY A, its employees or agents or by any of its customer or third party to the extent that such liability, loss, damage, injury, cost or expense was caused by, relates to or arises from the provision of the Services as a consequence of a direct or indirect breach or negligent performance or failure or delay in performance of this Agreement by the Service Provider.

13.2 It is not necessary for COMPANY A to incur expense or make payment before enforcing a right of indemnity conferred by this Agreement.

13.3 Without prejudice to the indemnities given COMPANY A shall promptly notify the Service Provider of any claim as soon as it becomes aware of such claim.

14 Record keeping and audit

14.1 Each Party shall maintain all material, financial and non-financial documentary records relating to this Agreement in a form which is reasonably accessible.

14.2 The Parties shall keep such documentary records as are required to be maintained by UAE regulatory requirements, applicable tax legislation or other applicable law or regulation for a further period of ten years after the end of the Term. After such period, each Party shall at its sole discretion either

(a) keep such documentary records for such periods as required by Regulatory Requirements, applicable tax legislation or other relevant laws or

(b) send such documentary records to (and at the cost of) the other Party.

14.3 Notwithstanding any other clause to the contrary in this Agreement, the Parties agree that COMPANY A or COMPANY A's representatives or nominees may from time to time audit the Service Provider's compliance with this Agreement from time to time. Such audit shall not take place more than four times in any year of this Agreement unless and to the extent COMPANY A reasonably believes that any additional audit is necessary in order to investigate:

(i) a material failure by the Service Provider's to perform its obligations under this Agreement;

(ii) a material miscalculation of the Fees and/or expenses; or

(iii) following a complaint which relates to any aspect of the Services.

14.4 COMPANY A or COMPANY A's nominee/representative shall notify details of the scope of and basis for any proposed audit to the Service provider at least 5 working days' prior to the intended date of such planned audit.

14.5 The Service Provider shall ensure that the relevant staff of COMPANY A, COMPANY A audit representatives, regulators and regulatory examiners acting in accordance with their supervisory powers under applicable law are allowed unrestricted access to the Service Provider, the Service Provider's premises, staff and documentary records as is required by such person to conduct required audits. The Service Provider shall promptly and efficiently give members of COMPANY A and COMPANY A Audit Representatives any assistance they reasonably require in connection with the exercise of their audit rights.

14.6 If the audit reveals that the Service Provider has not complied with any of its obligations under this Agreement, the Service Provider agrees and undertakes to act on and implement any

reasonable recommendations made by COMPANY A pursuant to the audit. If any audit reveals any overcharging by the Service Provider on any invCompany Ae, an appropriate correcting credit for the amount of the overcharge shall be made within fourteen (14) days of such overcharge being identified

15 Termination

15.1 The Agreement shall automatically and immediately terminate upon any one or more of the following events:

(a) either Party ceasing or threatening to cease to carry on business;

(b) dissolution or liquidation of either Party, save for the purpose of reconstruction or amalgamation; and/or

(c) insolvency or the Party or a received or a received and manager or judicial manager being appointed over either Party in respect of the whole or any part of its assets or if either Party makes an assignment for the benefit of or composition with its creditors generally or threatens to do so or any execution is levied against it which is not discharged within ten (10) days.

15.2 Either Party shall have the right to immediately terminate this Agreement by written notice of such termination to the other Party upon the happening of any of one or more of the following events:

(a) any sale, assignment or transfer (otherwise than in accordance with this Agreement) of any right, benefit or obligation under this Agreement by either Party without the prior written consent of the other Party hereto;

(b) fraud, gross negligence or wilful misconduct on the part of the other Party;

(c) any material breach or violation of any obligation contained in this Agreement by the other Party which, if capable of remedy, shall remain un-remedied for a period of thirty (30) calendar days after written notice thereof from the other Party or if such material breach or violation requires more than thirty (30) calendar days to remedy, if such steps are not commenced within thirty (30) calendar days and thereafter diligently executed; and/or

(d) the disability of either Party hereto, as a result of the law, regulation, guideline or rule applicable, directly or indirectly, to such Party, to perform in full any material obligation of such Party hereunder.

15.3 Notwithstanding anything mentioned to the contrary within this Agreement, COMPANY A may terminate this Agreement anytime and without any reason (for convenience) and without the need of any Court order, by giving the other Party not less than thirty (30) calendar day’s prior written notice. During such notice period, the Parties shall mutually cooperate to take necessary actions as the Parties deem appropriate to minimise disruption caused by such termination.

15.4 The termination of this Agreement shall not affect either Party's right in respect of any antecedent breach of this Agreement or any obligation or liability expressly stated herein to continue after termination.

16 Consequence of Termination

16.1 Termination of this Agreement in whole or in part for any reason shall be without prejudice to any rights which may have accrued up to the end of the Term. Rights to terminate this Agreement are not exclusive rights and shall be in addition to every other remedy or right now or hereafter existing.

16.2 In the event of Termination, COMPANY A shall be liable to pay all undisputed Service Fees as payable upto the effective date of termination.

16.3 Exit Assistance: The Service Provider agrees to provide COMPANY A with all reasonable assistance as may be required by COMPANY A to either enable (i) COMPANY A to resume services on its own; or (ii) should COMPANY A choose any alternate service provider then the Service Provider shall provide all assistance so as to enable the replacement service provider to continue the Services in an unobstructed manner. This includes but is not limited to transferring relevant data in the formats as required by COMPANY A, relevant manuals and process notes and/or any such other assistance to ensure seamless handover of the Services to COMPANY A or to such other service provider as may be appointed by COMPANY A.

17 Announcements

Except with the prior written consent of COMPANY A, the Service Provider shall not, and shall procure that no staff or member of the Service Provider shall make any public statement about the Services, this Agreement or otherwise publicise this Agreement or any information relating to it.

18 Notices

18.1 Any notice under this Agreement will be effective only if it is in writing.

18.2 Notice details for the parties are as follows:

Party	**Address and fax number**	**Addressee/marked for the attention of**
COMPANY A	P.O. Box 5209, Dubai +9714 233-7771	
Service Provider		

18.3 A Party may change its notice details for the purpose of this clause by giving notice to all the other parties in accordance with this clause

18.4 In proving the giving of a notice, it will be conclusive evidence to prove:

(a) if delivered by hand, that it was left at the relevant address; or
(b) if sent by post, that it was properly addressed and posted.

19 Relationship of the parties

19.1 Nothing in this Agreement shall be construed as creating the relationship of employer and employee and/or any partnership or joint venture between:

(a) the Service Provider and COMPANY A; or
(b) COMPANY A and any of the Service Provider's employees or representatives.

19.2 Except, and to the extent, that this Agreement expressly states otherwise, no Party may incur any expenses or negotiate on behalf of any other Party or commit any other Party in any way to any person without that other Party's prior written consent.

20 Entire agreement

20.1 This Agreement (together with all other documents to be entered into pursuant to it) sets out the entire agreement and understanding between the parties, and supersedes all proposals and prior agreements, arrangements and understandings between the parties, relating to its subject matter.

21 Amendments/VARIATION

21.1 No variation/amendment of this Agreement shall be effective unless it is in writing and signed by both the Parties.

22 Survival of rights

22.1 The termination or expiry of this Agreement for any reason shall not affect any rights or liabilities of eithat have accrued prior to such termination or expiry or the coming into force or continuance in force of any term that is expressly or by implication intended to come into or continue in force on or after termination or expiry.

23 Waiver

23.1 Failure by either Party to enforce any of the terms of this Agreement shall not in any way affect the validity of this Agreement nor prejudice that Party's right to take subsequent action.

23.2 Any waiver in connection with this Agreement shall, in any event, be only be effective if it is in writing, refers expressly to this clause, is duly signed by or on behalf of the Party granting it and is communicated to the other Party in accordance with clause (Notices).

24 Rights cumulative

24.1 The rights and remedies of the parties in connection with this Agreement are cumulative, are not exclusive of and may be exercised without prejudice to any other rights or remedies provided in this Agreement by law or equity or otherwise. Except as expressly stated in this Agreement (or in law or in equity in the case of rights and remedies provided by law or equity) any right or remedy may be exercised wholly or partially from time to time.

25 Severability

25.1 If any provision in this Agreement is or at any time becomes to any extent invalid, illegal or unenforceable under any enactment or rule of law, such provision will to that extent be deemed not to form part of this Agreement but the validity, legality and enforceability of the remainder of this Agreement will not be affected.

26 Counterparts

26.1 This Agreement may be entered into in the form of two or more counterparts, each executed by one or more of the parties but, taken together, executed by all and, provided that all the parties so enter into this Agreement, each of the executed counterparts, when duly exchanged and delivered, will be deemed to be an original, but, taken together, they will constitute one instrument. This Agreement may be circulated for signature through electronic transmission, including, without limitation via email, and all signatures so obtained and transmitted shall be

deemed for all purposes under this Agreement to be original signatures and shall have same legal effect as original wet signatures until such time, if ever, the original counterparts with original wet signatures are exchanged by the parties. No Party hereto shall raise the use of electronic mail attachment in “adobe acrobat pdf”, “docusign” or similar format(s) to deliver a signature, or the fact that any signature was electronically signed or transmitted or communicated as an attachment to an electronic mail message, as a defense to the formation of a contract and each party forever waives any such defense.

27 Anti-Bribery – Anti Corruption Provision

27.1 COMPANY A is required to act in accordance with the laws, regulations, and requests of regulatory authorities operating in applicable jurisdictions in which COMPANY A operates in, related amongst other things, to the prevention of anti-corruption, anti-money-laundering, sanctions and anti-terrorist financing. As a regulated entity, COMPANY A may at its sole discretion initiate any action it deems appropriate specifically in relation to this section or as a result of a request of regulatory authorities. Where appropriate and not prohibited by law, COMPANY A may keep the Service Provider informed regarding such actions if any initiated by COMPANY A.

27.2 The Service Provider represents to COMPANY A that it has not and agrees that it shall not in connection with the transactions contemplated by this Agreement, or in connection with any other business transactions involving COMPANY A, make any payment or transfer anything of value, offer, promise or give a financial or other advantage or request, agree to receive or accept a financial or other advantage either directly or indirectly to any other person or entity including any Government or regulatory entity or Government or regulatory employee, if it is not in compliance to UAE laws.

27.3 The Service Provider acknowledges and agrees that it is the clear and unambiguous intent of COMPANY A that in the course of its respective negotiations and performance of this Agreement no payments or transfers of value offers, promises or giving of any financial or other advantage or requests, agreements to receive or acceptances of any financial or other advantage shall be made either directly or indirectly which have the purpose or effect of public or commercial bribery or acceptance of or acquiescence in bribery, extortion, kickbacks, greasing or other unlawful or improper means of obtaining or retaining business, commercial advantage or the improper performance of any function or activity.

27.4 If fraud, bribery, corruption or any other form of wrongdoing is suspected based on reasonable grounds in relation to the procurement process or performance of any of its contracts or otherwise, such issue(s) must immediately be reported to COMPANY A on its ethics hotline number: +971-4-2337033 and/or by sending an email to: whistleblower@tameen.ae A dedicated team at COMPANY A will independently handle any reported violations.

27.5 The Service Provider agrees that all payments to the Service Provider will be suspended by COMPANY A immediately without penalty following written notification to the Service Provider, until such issue(s) has been investigated and cleared by COMPANY A. The Service Provider agrees to fully cooperate with COMPANY A’s investigation process.

27.6 Where fraud, breach of this clause or any other wrongdoing is established, COMPANY A may at its own sole discretion exercise its right to terminate its contract immediately and without limitation to any other rights and remedies available to COMPANY A including to further initiate appropriate legal action

28 Taxes:

28.1 The Fees and/or Charges payable for the supply of services/goods stated under this agreement are shown exclusive of any Value Added Tax (VAT) or any other similar taxes, charges or duties to the extent any such tax is applicable or will become applicable as a result of provision of the services.

VAT for the purpose of this Agreement shall mean any value added tax imposed under or pursuant to the UAE Federal Decree-Law No. 8 of 2017 on Value Added Tax and the Cabinet Decision No. 52 of 2017 on the Executive Regulations of the Federal Decree-Law No. 8 of 2017 on Value Added Tax as amended or substituted from time to time.

28.2 COMPANY A reserves the right to withhold payment in case the Service Provider/Supplier does not issue a valid tax InvCompany Ae as required under the relevant VAT Laws. Payment will be made only after the receipt of valid Tax invCompany Ae and related documents. Any consequences arising from not receiving the valid tax invCompany Ae (including within required time frame) shall be Service Provider/Supplier's responsibility.

28.3 In case the relevant Tax Authority does not treat the invCompany Aes submitted as valid tax invCompany Aes, the Service Provider/Supplier agrees to issue revised valid tax invCompany Aes within a reasonable period, failing which COMPANY A reserves the right to adjust the invalid invCompany Ae amounts against subsequent payments.

28.4 Tax invCompany Ae and related documents shall be submitted in reasonable time (as specified in law).

28.5 In case there is a self-billing agreement between the Service Provider/Supplier and COMPANY A,COMPANY A during the term of such agreement shall then be responsible for issuing "Tax invCompany Ae raised by buyer/Tax credit note created by buyer" in relation to the transaction on behalf of the Supplier/ Service Provider provided that the Supplier/Service Provider is obligated to immediately review the tax invCompany Ae so received from the Customer and report to the Customer any discrepancy/errors within five calendar days of receiving the tax invCompany Ae as raised by the Customer.

29 Governing Law & Jurisdiction

(a) This Agreement will be governed by and construed in accordance with the laws of the Dubai, United Arab Emirates, and all claims and disputes between the parties or any of them arising out of or in connection with this Agreement will be determined in accordance with laws of Dubai, United Arab Emirates Law (which for avoidance of doubt excludes laws of DIFC).

(b) Each Party submits to the exclusive jurisdiction of the Courts of Dubai as established under Law No. (3) of 1992 (Establishing the Courts of the Emirate of Dubai and its related amendment(s) (which for avoidance of doubt excludes DIFC Courts) in relation to all claims, disputes, differences or other matters arising out of or in connection with this Agreement.

(c) Each Party irrevocably waives any right that it may have to object on any ground to an action being brought in the above referred court of Dubai, to claim that the action brought in the above Courts of Dubai (i.e. excluding DIFC Courts) has been brought in an inconvenient forum or to claim that the Courts of Dubai do not have jurisdiction and to oppose the enforcement of any judgment of any Court of Dubai.

(d) The Parties agree in the event of any dispute between the Parties, each Party will continue to perform its obligations under the Agreement during the resolution of such dispute, except for the obligations that may be the subject matter of such dispute.

Signed by the Parties or their duly authorised representatives on the date of this Agreement.

Signed by	)	.....
duly authorised for and on behalf of	)	
Company A (COMPANY A)	)	.....

Signed by	)	.....
duly authorised for and on behalf of	)	
[Service Provider]	)	.....

Schedule 1

The Services:

The Service Provider shall provide services related to :

Schedule 2

Service Fees

COMPANY A shall pay the below Service Fees to the Service Provider

SCHEDULE 3

THIRD PARTY – SECURITY/PRIVACY BEST PRACTICES REQUIREMENTS PRESCRIBED BY COMPANY A

Cooperation is the key to success. At COMPANY A, we believe that working with third parties helps businesses increase their productivity and efficiency, produce better products and services, employ highly qualified experts, and cut costs. But all these benefits come at the price of increased cybersecurity risks. Minor flaws in partner's security and privacy routines may turn into cybersecurity weaknesses and may be detrimental to the interests of both parties. As per this document, we convey to our partners/suppliers about minimum security best practices that needs to be followed to mitigate cybersecurity and privacy related risk which shall be beneficial for both parties.

1. Scope

Supplier/Vendor (hereinafter termed as Supplier in this document) should comply Information Security and Privacy related best practices termed as Company A's (COMPANY A) information security requirements as set forth these third-party security requirements. This Security requirement document applies to Supplier's performance under all prospective and existing agreements and all Processing of, and Security Incidents (including privacy or personal data related incidents) involving, COMPANY A Information. This Security requirement document does not limit other obligations of Supplier, including under the Agreement or laws that apply to Supplier, Supplier's performance under the Agreement, or the Permitted Purpose. To the extent these Security requirements conflicts with the Agreement, Supplier will promptly notify COMPANY A of the conflict and will comply with the requirement that is more restrictive and protective of COMPANY A Information (which may be designated by COMPANY A). These commitments apply to Supplier and its Personnel.

2. Definitions

- The following definitions apply to this Security requirement document**:**
- **"Aggregate"** means to combine or store COMPANY A Information with any data or information of Supplier or any third party.
- **"COMPANY A Information"** means: (a) all Company A (COMPANY A) Confidential Information (as defined in the existing/prospective Agreement or in the non-disclosure agreement between the parties); (b) all other data, records, files, content, or information received from COMPANY A or its affiliates and Processed by Supplier in connection with the Agreement; and (c) data derived from (a) or (b), even if Anonymized**.**
- **"Confidentiality, Integrity, and Availability"** refers to the three properties of the information-security model known as the "CIA Triad." Confidentiality is the property that data or information is not made available or disclosed to unauthorized persons or processes. Integrity is the property that data or information have not been altered or destroyed in an unauthorized manner. Availability is the property that data or information is accessible and useable upon demand by an authorized person.
- **"Personnel"** means Supplier's or Subcontractor's employees, agents, subcontractors, and other authorized users of its systems and network resources.
- **"Physical, Administrative, and Technical Safeguards"** refers to the controls an organization implements to maintain information security. Physical safeguards address physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. Administrative safeguards address administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic data or

information and to manage the conduct of Personnel in relation to the protection of that data or information. Technical safeguards address the technology, and the policies and procedures for its use, that protect electronic data or information and control access to it.

- **"Process"** means to perform any operation or set of operations on data, such as access, use, collection, receipt, storage, alteration, transmission, dissemination or otherwise making available, erasure, or destruction.

3. Permitted Purposes

Supplier will Process COMPANY A Information only as follows (each, a "**Permitted Purpose**"):

a) **Authorized data.** Supplier may Process only the COMPANY A Information expressly authorized under the Agreement. If there is no express authorization, the Supplier may process only the COMPANY A Information necessary to perform the services under the Agreement.

b) **Only for purposes expressly authorized.** Supplier may Process COMPANY A Information only for purposes expressly authorized under the Agreement.

c) **Sale or other transfer prohibited.** Supplier will not transfer, rent, barter, trade, sell, loan, lease, or otherwise distribute or make any COMPANY A Information available to any third party, other than the authorized purposes.

d) **Data aggregation prohibited.** Supplier will not Aggregate COMPANY A Information, even if anonymized or pseudonymized, except as expressly authorized under the Agreement

4. Information Security Requirements

A. **General Security Requirements**: Supplier will maintain Physical, Administrative, and technical safeguards consistent with industry-accepted best practices [(including the International Organization for Standardization's standards ISO 27001 and 27002, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NESA, or other similar industry standards for information security)] to protect the Confidentiality, Integrity, and Availability of COMPANY A Information.

a) **Specific Safeguard Requirements**: In addition to following the above standards, Supplier's information security program will include, at a minimum, the following safeguards, and controls:

b) **Written information security policy and program**. Supplier shall implement a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

c) **Security awareness training**. Supplier will provide periodic security training to its Personnel on relevant threats and business requirements

d) **Data inventory**. Supplier will document and maintain information regarding how and where COMPANY A Information is Processed while in Supplier's possession or control.

e) **Secure configurations**. Supplier shall manage security configurations of its systems using industry best practices to protect COMPANY A Information from exploitation through vulnerable services and settings.

f) **Controlled use of administrative privileges**. Supplier shall limit and control the use of administrative privileges on computers, networks, and applications consistent with industry best practices.

g) **Vulnerability and patch management**. Supplier will maintain a process to timely identify and remediate system, device, and application vulnerabilities through patches, updates, bug fixes, or other modifications to maintain the security of COMPANY A Information.

h) **Maintenance, monitoring, and analysis of audit logs**. Supplier will collect, manage, retain, and analyze audit logs of events to help detect, investigate, and recover from unauthorized activity that may affect COMPANY A Information as per legal requirements.

i) **Malware defenses.** Supplier will deploy anti-malware software [to and configure all workstations and servers on Supplier's network] to control and detect the installation, spread, and execution of malicious code.

j) **Firewalls**. Supplier will maintain and configure firewalls to protect systems containing COMPANY A Information from unauthorized access. Supplier will review firewall rule sets at least annually to ensure valid, documented business cases exist for all rules.

k) **Suitable Environment**. Data will be used in an environment suitable to its purpose. Production data will not be used on test equipment and test data will not be used on production equipment.

l) **Change Management**. Changes to production systems are tracked, recorded, and reviewed.

m) **Disablement of services**. Disable all unnecessary services, protocols, and ports and allow only Authorized services

n) **Encryption**. Supplier will encrypt all COMPANY A Information at rest and when in transit across open networks in accordance with industry best practices. Upon COMPANY A written request, the supplier will confirm that all copies of encryption keys have been securely deleted.

o) **Access controls**. Supplier will implement the following access controls with respect to COMPANY A Information:

i. Unique IDs. Supplier will assign individual, unique IDs to all Personnel with access to COMPANY A Information, including accounts with administrative access. Accounts with access to COMPANY A Information must not be shared.

ii. Need-to-know. Supplier will restrict access to COMPANY A Information to only those Personnel with a "need-to-know" for a Permitted Purpose.

iii. User access review. Supplier will periodically review Personnel and services with access to COMPANY A Information and remove accounts that no longer require access.

p) **Account and password management.** Supplier will implement account and password management policies to protect COMPANY A Information, including, but not limited to:

i. No default passwords. Before deploying any new hardware, software, or other asset, Supplier will change all default and manufacturer-supplied passwords to a password consistent with the password strength requirements in subsection 0 (iii).

ii. Inventory of administrative accounts. Supplier will maintain an inventory of all administrator accounts with access to COMPANY A Information and will provide a list of these accounts to COMPANY A at COMPANY A's request.

iii. Password strength. Supplier will ensure that all Personnel use strong passwords by enforcing the following minimum requirements:

- passwords must be a minimum length of 8 characters.
- passwords may not match commonly used, expected, or compromised passwords; and
- Supplier must force a password change if there is evidence the password may have been compromised.
- Supplier will enforce sufficient password history controls

iv. Credential encryption. Encrypted passwords and other secrets shall be stored in an industry-accepted form that is resistant to offline attacks.

v. Rate limiting. Supplier shall implement an industry-accepted rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on a user's account.

q) **Remote access:** multi-factor authentication required. Supplier will implement multi-factor authentication, wherever required to secure COMPANY A Data/information.

r) Data segregation. Except where expressly authorized by COMPANY A in writing, Supplier will always logically [and physically] isolate COMPANY A Information from Supplier's and any third-party information**.**

s) **Security testing.** Supplier will conduct periodic internal and external penetration testing of systems that Process COMPANY A Information to identify vulnerabilities and attack vectors that can be used to exploit those systems. Identified vulnerabilities shall be addressed as part of Supplier's vulnerability management program.

t) **Personnel security and nondisclosure.** COMPANY A may condition access to COMPANY A Information by Supplier Personnel on Supplier Personnel's execution and delivery to COMPANY A of individual nondisclosure agreements, the form of which is specific by COMPANY A. [If requested by COMPANY A, Supplier will obtain and deliver to COMPANY A signed individual nondisclosure agreements from Supplier Personnel that will have access to COMPANY A Information before granting access to Personnel.]

u) **PCI DSS requirements. If**, during its engagement by COMPANY A, Supplier has access to or will Process credit, debit, or other payment cardholder information, Supplier shall always remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS")

5. Privacy Requirements

a) Supplier shall maintain a professional privacy policy duly complying with the applicable global and local regulatory requirements/expectations.

b) Supplier shall maintain record of processing activities involving privacy data (Personally identifiable data and Protected Health information or any other sensitive data of COMPANY A and its clients.

c) Supplier shall implement appropriate privacy protection solutions/controls including process related controls.

d) Supplier shall provide privacy awareness training to its employees included contract resources and third-party resources.

6. Subcontracts

Except as expressly set forth in the existing/prospective Agreement, Supplier will not subcontract or delegate any of its obligations under this Security Policy to any subcontractors, affiliates, or delegates ("Subcontractors") without COMPANY A's prior written consent.

7. Access to COMPANY A Extranet and Supplier portals

COMPANY A may grant Supplier Personnel access to COMPANY A Information via web portals or other non-public websites or extranet services on COMPANY A's or a third party's website or system (each, an "Extranet") for the Permitted Purposes. If COMPANY A permits Supplier to access any COMPANY A Information using an Extranet/public portal and supplier must comply with the following requirements:

a) ***Permitted Purpose.*** Supplier and its personnel will access the Extranet and access, collect, use, view, retrieve, download or store COMPANY A Information from the Extranet solely for the Permitted Purpose.

b) ***Accounts.*** Supplier will ensure that Supplier Personnel use only the Extranet account(s)/access to COMPANY A system remotely by designated resources and sensitize their personnel to keep their access credentials confidential. Accounts are not to be shared.

c) ***Systems.*** Supplier will access the Extranet only through computing or processing systems or applications running operating systems managed by Supplier viz. supplier company provided laptop/desktop, network equipment. All such systems shall be subject of host validations like checking latest patch level, AV update, MAC etc. by COMPANY A, wherever required.

d) ***Restrictions***. Except if approved in advance in writing by COMPANY A, Supplier will not download, mirror, or permanently store any COMPANY A Information from any Extranet on any medium, including any machines, devices, or servers.

e) ***Account Termination***. Supplier will terminate the account of each of Supplier's personnel and notify COMPANY A no later than 24 hours after any specific Supplier personnel who has been authorized to access any Extranet (a) no longer needs access to COMPANY A Information or (b) no longer qualifies as Supplier personnel (e.g., the personnel leaves Supplier's employment). Suppliers who are managing access as part of MSSP are to adhere this guideline on their own.

8. Data Retention, Return, and Destruction

a) Retention. Supplier will retain COMPANY A Information only as necessary for the Permitted Purposes.

b) ***Return and secure deletion of COMPANY A Information.*** At any time during the term of the Agreement at COMPANY A's request, or upon the termination or expiration of the Agreement for any reason, Supplier shall, within 5 business days (or 30 calendar days for data in backup or online storage), return to COMPANY A and securely delete all copies of COMPANY A Information in its possession or control. Supplier shall confirm in writing that all copies of COMPANY A Information have been returned and securely deleted.

c) ***Archival copies.*** If Supplier is required by law to retain archival copies of COMPANY A Information for tax or similar regulatory purposes, Supplier shall (i) not use the archived information for any other purpose; and (ii) remain bound by its obligations under this agreement, including, but not limited to, its obligations to protect the information using appropriate safeguards and to notify COMPANY A of any Security Incident involving the information.

9. **Deletion standard**

All COMPANY A Information deleted by Supplier will be securely deleted using an industry-accepted practice designed to prevent data from being recovered using standard disk and file recovery utilities (e.g., secure overwriting, degaussing of magnetic media, shredding, or mechanical disintegration). With respect to COMPANY A Information encrypted in compliance

with these requirements, Supplier may delete data by permanently and securely deleting all copies of the encryption keys.

10. **Media destruction**

Before permanently discarding or disposing of storage media that (1) Supplier has physical access to or control of (e.g., laptop hard drives, desktop hard drives, USB or "thumb" drives, backup media, hard drives used in the Supplier's own data center, or other portable storage media) and (2) contains, or has at any time contained, COMPANY A Confidential Information, Supplier will destroy the storage media using a technique designed to render the media unusable and the data unrecoverable (e.g., disintegration, incineration, pulverizing, shredding, and melting). This section shall not apply to storage media that Supplier does not have physical access to or control of, such as storage media used in a public cloud or other third-party environment. In such cases, Supplier shall ensure that all COMPANY A Confidential Information stored in the third-party environment is securely deleted when no longer needed using an industry-accepted practice (see Section 9 - Deletion standard).

11. Security Reviews and Audits

a. ***Vendor assessment questionnaires.*** Upon COMPANY A's request, Supplier will complete a new COMPANY A risk assessment questionnaire.

b. ***Compliance with agreement.*** Upon COMPANY A's request, Supplier will confirm in writing to COMPANY A Supplier's compliance with this Agreement.

c. ***Other reviews; audits.*** Upon COMPANY A's written request, to confirm Supplier's compliance with this Agreement, Supplier grants COMPANY A or, at COMPANY A's election, a third party on COMPANY A's behalf, permission to perform an assessment, audit, examination, or review of the Physical, Administrative, and Technical Safeguards in place to protect COMPANY A Information Processed by Supplier under the Agreement. Supplier shall fully cooperate with the assessment.

d. ***Remediation.*** Supplier will promptly address any exceptions or deficiencies identified during COMPANY A's security review or in any audit report, by developing and implementing a corrective action plan agreed to by Supplier and COMPANY A, at Supplier's sole expense.

12. Security Incidents

a. ***Security Incident defined.*** *A "Security Incident" is (i) any actual or suspected compromise of the Confidentiality, Integrity, or Availability of COMPANY A Information; (ii) any actual or suspected compromise of, or unauthorized access to, any system that Processes COMPANY A Information that presents a risk to the Confidentiality, Availability, or Integrity of COMPANY A Information; or (iii) receipt of a complaint, report, or other information regarding the potential compromise or exposure of COMPANY A Information Processed by Supplier.*

b. ***Incident response plan***. Supplier shall maintain a written incident response plan and provide a copy of the plan to COMPANY A upon request. Supplier will remedy each Security Incident in a timely manner following its response plan and industry best practices.

c. ***Notice required.*** Supplier will notify COMPANY A of any Security Incident within 72 hours of becoming aware of the Security Incident.

d. ***Cooperation with COMPANY A's investigation***. Supplier will reasonably cooperate with COMPANY A in COMPANY A's handling of a Security Incident, including, without limitation: (i) coordinating with COMPANY A on Supplier's response plan; (ii) assisting with COMPANY A's

investigation of the Security Incident; (iii) facilitating interviews with Supplier's Personnel and others involved in the Security Incident or response; and (iv) making available all relevant records, logs, files, data reporting, forensic reports, investigation reports, and other materials required for COMPANY A to comply with applicable laws, regulations, or industry standards, or as otherwise required by COMPANY A.

e. ***Third-party notifications.*** Supplier agrees that it shall not notify any third party (including any regulatory authority or customer) of any Security Incident on behalf of COMPANY A without first obtaining COMPANY A's prior written consent. Further, Supplier agrees that COMPANY A shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, or others; and (ii) the form and contents of such notice.

13. Notice of Legal Process

Supplier will inform COMPANY A within 72 hours when COMPANY A's data is being sought in response to legal process or other applicable law or within reasonable advance period to action on underlying request.