cora

Subscription Services Agreement

July | 2023

The Power of Perspective

Subscription Services Agreement

THIS PAGE WAS LAST UPDATED JULY 25TH 2023. FOR PRIOR VERSIONS OF THIS AGREEMENT SEE THE ARCHIVE AT https://corasystems.com/agreements-and-terms/subscription-services-agreement/

THIS SUBSCRIPTION SERVICES AGREEMENT ("AGREEMENT") GOVERNS THE USE OF THE SAAS AND SERVICES THAT CUSTOMER IS PROCURING FROM CORA SYSTEMS LIMITED AND/OR ITS AFFILIATES OR SUBSIDIARIES ("CORA"). BY EXECUTING A SALES ORDER AND/OR BY USING THE APPLICABLE SAAS OR SERVICES, THE ENTITY EXECUTING THE APPLICABLE ORDER ("CUSTOMER") AGREES THAT THE TERMS OF THIS AGREEMENT GOVERN, AGREE THAT IT IS AUTHORIZED TO BIND THE APPLICABLE ENTITY TO THIS AGREEMENT AND IS AGREEING TO BE BOUND BY THE TERMS CONTAINED IN THIS AGREEMENT. CUSTOMER SHOULD NOT USE THE SAAS AND/OR SERVICES IF IT CANNOT COMPLY WITH THIS AGREEMENT.

1.   Terms of Engagement

Cora and the Customer have agreed that, for the duration of the Subscription Term, the Customer shall engage Cora to provide access to its SaaS solution and related services in accordance with the terms of this Agreement in consideration of the payment by the Customer of the fees.

2.   Sales Order

Customer may order the Services by executing a Sales Order which shall indicate any subscriptions, and Professional Services being ordered and the associated fees. The Sales Order is effective on the date of last signature and except as otherwise provided in this Agreement, the Sales Order, or a SOW, Sales Orders are non-refundable and non-cancellable.

3.   Subscription

a) During the Subscription Term and subject to the terms and conditions of this Agreement, Customer may access and use the elements of the SaaS and Services which the Customer has ordered on a limited, non-exclusive, worldwide basis. Cora retains all right, title, and interest in and to the Services, including all software included in and used to provide the SaaS and all logos, trademarks and Cora branding reproduced in the SaaS. The Customer shall not have any other right to the SaaS that is not specifically set forth in this Agreement.

b) Cora reserves the right to implement new versions and upgrades of the SaaS including changes to the design, operational method, technical specifications, systems, and other functions, at any time without prior notice. The rights and obligations provided in this clause and elsewhere in this Agreement shall apply to any future upgrades and updates to the SaaS.

a) Customer may access and use the SaaS solely for its internal business purposes, during the Subscription Term, and in accordance with the number of Users indicated on the Sales Order. Customer may provide Users with access to the SaaS and acknowledges Customer shall be fully liable for its Users compliance with this Agreement.

4. Restrictions

a) The Customer has no right (and shall not permit any agents or other third party) to reproduce, modify, distribute, disassemble, decompile, reverse engineer, or publicly display or perform the software included in the SaaS.

b) Customer may not license, sell, transfer, assign, distribute, outsource, translate, localize, adapt, rent, lease, loan, prepare derivative works of, or otherwise commercially exploit or make the SaaS available to any third party except as permitted by this Agreement or a Statement of Work or Sales Order.

c) Customers and Users may not access the Services if they are a direct competitor to Cora, except with Cora's prior written consent. Customer is not permitted to access the Services for purposes of monitoring its performance, functionality, or availability, or for any other benchmarking or competitive purposes or perform or disclose network discovery, vulnerability scanning, password cracking, or penetration testing of the Services. Customer may not perform or fail to perform any act which would result in a misappropriation or infringement of Cora's (or its supplier's) intellectual property rights in the SaaS, its components, or related documentation.

5. Supplier Duties

a) Cora will support and maintain the SaaS for the Customer in accordance with the Service Level and Support Objectives [https://corasystems.com/wp-content/uploads/2022/06/Service-Level-and-Support-Objectives-June-2022.pdf].

b) During the Subscription Term, Cora will meet the Service Level and Support Objectives which are hereby incorporated into this Agreement.

6. Fees and Payment

a) The Customer will pay the fees that are indicated in the Sales Order.

b) Unless the Sales Order provides otherwise, invoices shall be due upon receipt. The Customer will issue a purchase order for the initial year promptly following execution of the Sales Order. The validity of a license key is subject to the annual receipt of payment prior to the Subscription Start Date and each subsequent anniversary. The invoiced amount shall be payable by electronic transfer to the bank account listed on the invoice and in the currency listed on the invoice.

c) Unless the Sales Order provides otherwise Professional Services, where applicable, will be invoiced separately and payment will be due upon receipt.

d) All fees are non-refundable except as otherwise explicitly stated in the Sales Order or this Agreement.

e) On each anniversary of the Subscription Start Date, the fees shall be subject to an uplift in line with Cora's then standard pricing.

f) Interest on overdue payments shall be payable in accordance with law and Cora reserves the right to charge a fee for any payment reminders. Customer shall be responsible for the reasonable costs Cora incurs when collecting overdue fees. In any event, all fees must be paid prior to termination.

g) Without limiting its other rights, if Customer fails to pay overdue payments after Cora has provided 2 delinquency notices and at least twenty days have passed since the first notice, then Cora may suspend the Customer's access to the SaaS. If payments are more than fifty days overdue, Cora may immediately terminate this Agreement, terminate the Subscription, and delete the Customer Data. In the event of

early termination of the Agreement under this Clause 6G, the Customer shall not be entitled to a refund of any prepaid fees.

h) All sums payable under this Agreement are exclusive of Value Added Tax, Sales Tax, Withholding Taxes, and any local taxes, levies, or duties which are to be paid by the Customer. Cora is responsible only for taxes based on Cora's income and if Cora is obliged by law to pay taxes for which Customer is responsible under this clause, Cora may invoice this amount to Customer.

i) The Customer may, at any time, increase the number of Users or upgrade the support services. The Customer is not permitted to reduce the number of Users. Any additional Users and/or additional capacity or functionality procured during the Subscription Term shall be coterminous with pre-existing Service and will co-terminate with and be prorated through the end date of the Subscription Term for the applicable Service.

j) The Customer shall bear the cost of any travel, expenses or costs that may be incurred by Cora to provide the Services, save with the written consent of Cora.

7. Intellectual Property

a) As between the parties, the Customer acknowledges that all Intellectual Property Rights, title, and interest in and to the SaaS, all components, software and copies thereof and all customisation, derivations, and configuration developed from the SaaS shall remain vested in Cora. Any rights in the Services or Cora's intellectual property that are not expressly granted herein are reserved by Cora.

b) As between the parties, Cora acknowledges and agrees that all title and interest in the Customer Data shall remain vested in the Customer. Customer grants Cora the right to store, host, process, use, maintain, transmit, and perform any other function on the Customer Data for the purpose of providing the Services. Following termination or expiration of this Agreement, Cora shall be entitled to deactivate the Customer account and delete any Customer Data in accordance with its deletion procedures. Customer is responsible for the accuracy, integrity, and lawfulness of Customer Data and for obtaining any rights necessary for Cora's performance of the Services.

c) Cora shall own all right and title to any anonymized, aggregated or de-identified data that is derived from the Customer Data.

8. Confidential Information

a) In this Agreement "**Confidential Information**" means all information disclosed (whether in writing, orally or by any other means and whether directly or indirectly and whether specifically designated as 'confidential' or which ought reasonably be regarded as confidential) under or in connection with this Agreement by one party (the "**Disclosing Party**") to the other party (the "**Receiving Party**") whether before or after the date of this Agreement including, without limitation, information relating to the Disclosing Party's products, services, operations, processes, plans or intentions, product information, know-how, pricing, design rights, trade secrets, market opportunities and business affairs.

b) During the Subscription Term and after termination of this Agreement for any reason the Receiving Party:

    a. will not use Confidential Information for a purpose other than the performance of its obligations under this Agreement;

b. will not disclose Confidential Information to a person except with the prior written consent of the Disclosing Party or as permitted herein; and

c. shall make every effort to prevent the unauthorized use or disclosure of Confidential Information.

c) During the Subscription Term the Receiving Party may disclose Confidential Information to any of its directors, officers, employees, affiliates, contractors, employees and contractors of affiliates, legal and business advisors (a "**Recipient**") to the extent that disclosure is reasonably necessary for the purposes of this Agreement provided that the Receiving Party shall ensure that a Recipient is made aware of the Receiving Party's obligations of confidentiality under this Agreement. The Receiving Party shall be liable for Recipient's compliance with this Agreement.

d) Confidential Information does not include information that (i) is in the Receiving Party's lawful possession at the time of disclosure; (ii) is independently developed by Recipient without use of or reference to Confidential Information; (iii) becomes known publicly, before or after disclosure, other than as a result of Receiving Party's improper action or inaction, or breach of this Agreement; or (iv) is approved for release in writing by the Disclosing Party.

9. Professional Services

This Clause 9 shall apply only if one or more Professional Services are indicated in the Sales Order or the parties have entered into a SOW.

a) If applicable, Cora shall use the Customer's equipment in accordance with any applicable permissions or third-party licences which have been notified to it in writing in advance.

b) If applicable, any training should be taken advantage of no later than six (6) months after the date of the Sales Order.

c) If training is to take place in person, then Customer is responsible for providing an appropriate location for training to take place as well as a computer connected to a projector and the internet. Customer is also responsible for inviting participants and ensuring they are present.

d) Where applicable, Cora shall take all reasonable care to ensure that, in performing any Professional Services, it does not cause outage to the Customer's production environment and/or disrupt operations.

10. Change Management Process

a) Any material change to the Services that may be requested by the Customer (the "**Change(s)**") shall be dealt with in accordance with the following procedure:

b) the Customer will provide Cora with a written request detailing the proposed Change (the "**Change Request**") and as soon as possible following receipt of a Change Request Cora will provide the Customer with a Statement of Work detailing the implications of the proposed Change and a breakdown of the associated costs.

c) the Customer must then notify Cora within thirty (30) Business Days if it wants to proceed with the Change whereby Cora will carry out the Change.

11. Subcontractors

Cora may retain subcontractors, including third party software suppliers, for the performance of obligations under this Agreement provided that Cora shall remain liable for the work of any subcontractors in the same manner as for its own work.

12. Chain of Communication

The Account Contact as indicated on the Sales Order shall be Cora's primary point of contact, for the purposes of this Agreement (except where otherwise provided). The Customer may change the Account Contact, at any time during the Subscription Term, by notice in writing.

13. Security

a) Cora shall maintain commercially reasonable measures for ensuring the security of the SaaS meets relevant industry standards. These shall include physical, administrative and technical safeguards for the protection, integrity, and confidentiality of Customer Data as described in the Security Policy [https://corasystems.com/wp-content/uploads/2022/04/Cora-Security-Policy.pdf] as applicable from time to time which can be found on the Website.

b) Customer recognizes its use of the SaaS will involve transmission of Customer Data over the internet and networks, some of which may not be owned and operated by Cora. Without limiting Cora's security, confidentiality, and data protection obligations provided herein, Cora is not responsible for Customer Data that is lost, intercepted, altered or otherwise compromised during the transmission of data across networks not owned or operated by Cora, including the internet and Customer's own network. The Customer acknowledges that Customers access to the Internet cannot be guaranteed, and Cora shall not be liable for deficiencies in the Customers own equipment or Internet connections.

14. Terms of Service

a) The Customer will co-operate to the fullest extent necessary to enable Cora to replicate any issues to determine that an issue resides with the SaaS, and to certify that the issue is corrected when necessary.

b) Except with written permission from Cora, Customer shall not use the SaaS to store, transmit or process data that is subject to industry specific regulations or otherwise sensitive including credit card information, social security data, protected health information (as defined in the Health Insurance Portability and Accountability Act of 1996 "HIPAA"), International Traffic in Arms Regulations ("ITAR") related data, data classified or used on the U.S. Munitions list, or special categories of personal data (as defined in the GDPR).

c) Cora monitors the SaaS and Services in order to resolve Customer technical assistance requests, detect and address threats to the security, availability, and functionality of the SaaS. Cora may collect usage data and use such data in an aggregated form and compile statistical and other information related to the performance of the Services for purposes of improving Cora's products and services.

d) Customer and Customer's Users may not use the SaaS and Services (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate the rights of others; (iii) to try to gain unauthorized access to or disrupt any service, device, data, account or network; (iv) to spam or distribute malware; (v) in a way that could harm the SaaS or impair anyone else's use of it; (vi) in any application or situation where failure of the SaaS could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage, except in accordance with the High-Risk Use

terms in clause 14(e) below; (vii) to store or transmit material that infringes upon any third party's intellectual property rights; or (viii) to assist of encourage anyone to do any of the above.

e) Customer acknowledges that modern platform technologies, may be used in new and innovative ways, and Customer must consider whether its specific use of these technologies is safe. The SaaS is not designed or intended to support any use in which a service interruption, defect, error, or other failure of the SaaS could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "High-Risk Use"). Accordingly, Customer must use and implement the SaaS such that, in the event of any interruption, defect, error, or other failure of the SaaS, the safety of people, property, and the environment are not reduced below a level that is reasonable, appropriate, and legal, whether in general or for a specific industry. Customer's High-Risk Use of the SaaS is at its own risk. Cora, its affiliates and suppliers will not be liable to Customer in any way for use of the SaaS in a high risk environment. Customer agrees to defend, indemnify and hold Cora harmless from and against all damages, costs and attorneys' fees in connection with any claims arising from a High-Risk Use associated with the SaaS, including any claims based in strict liability or that Cora was negligent in designing or providing the SaaS to Customer. The foregoing indemnification obligation is in addition to any defense obligation and is not subject to any limitation of liability.

f) Cora may suspend Customer's access to the SaaS and Services or any part thereof on the following grounds: (a) late payment/non-payment of undisputed fees; (b) non-renewal of the Services by Customer; (c) Customer's or its Users' breach of the Agreement; (d) in the event suspension is deemed necessary by Cora to prevent or address the introduction of malicious software, a security incident, or other harm to Customer, Cora, or Cora's other customers. Cora will notify Customer of any such suspension and will endeavour to limit, where commercially feasible, the suspension to affected Users or technology, and will restore the availability of the same as soon as the issues leading to the suspension are resolved. Such suspension will in no way affect Customer's other obligations under this Agreement.

15. Passwords

a) The Customer shall ensure passwords provided in the registration process are securely stored and will ensure they are not accessed by third parties. The Customer shall be liable for any unauthorized use of the SaaS and Cora shall have no liability for damage arising from the Customer's failure to secure passwords.

b) The Customer shall immediately notify Cora if a password is lost or compromised, if an unauthorized party learns the password, or if one of these events is suspected to have occurred. In these cases, Customer shall immediately change the password in question.

c) Where Customer intentionally or negligently reveals a user password/identity to a third party or it becomes known to a third party through some other avenue, Customer shall be liable to Cora for any loss or damage incurred by Cora unless Customer immediately notifies Cora upon suspicion that such an event has occurred.

16. Customer Obligations

The Customer shall notify Cora of any breach or suspected breach of the following Customer obligations:

a) Customer shall comply with any security and administrative policies that are notified to it in relation to its use of the SaaS during registration, by email, or through posting on the Website.

b) Customer shall ensure any contact and billing information provided in relation to this Agreement is correct and undertakes to update such information promptly if and when any change to such information occurs.

c) Customer recognizes a User account may not be shared and is intended for use by only one individual User.

d) Customer shall remain liable for the Users use of the SaaS and shall ensure User's compliance with this Agreement. To the extent Customer is unable to prevent unauthorized use or cause a User to perform an obligation it owes to Cora, or otherwise to perform such obligation on the Users behalf, then the Customer shall indemnify Cora for any loss relating to such unauthorized use or non-performance by the User of its obligations to Cora.

e) Customer is solely responsible for the lawfulness of the Customer Data including any content which is uploaded to, processed, entered into, or transferred through the SaaS by the Customer or its Users. Customer shall be responsible for monitoring its Customer Data and shall be liable to Cora for ensuring it is lawful and non-infringing of third-party rights.

17. Personal Data

a) The Customer acknowledges Users shall provide personal information in order to access and use the SaaS.

b) To the extent Cora is considered to be a processor in relation to the Services, Cora shall fulfil its obligations in this regard in accordance with the GDPR and the Data Protection Act 2018 ("DPA") and also accepts such assignment based on the instructions, terms and conditions in the SSA and the Cora Data Protection Appendix ("CDPA") [https://corasystems.com/wp-content/uploads/2022/04/Cora-Data-Protection-Appendix.pdf] which is hereby incorporated into this Agreement.

c) The Customer shall, in relation to its use of the Services, at all times process personal data in accordance with applicable data protection laws and regulations. Where Customer is considered to be a Data Controller within the meaning of the General Data Protection Regulation ("GDPR") in its use of the Services, Customer shall in such event have the sole responsibility for the accuracy, quality, and legality of personal data and the means by which it was acquired.

d) Customer recognizes Cora's mobile app and web page is freely accessible to Customer's Users and control over locations from which the app may be accessed lies with the Customer and not with Cora. Customer shall be responsible for authorization and management of User accounts across geographies including as relevant to transfer of Customer data and any relevant export controls.

18. Warranties and Remedies

a) Each party represents that it has validly entered into this Agreement with full power and authority.

b) Cora warrants to the Customer that during the Subscription Term (i) the Customer's production instance shall conform in all material respects with the Documentation, and (ii) Cora shall perform any Professional Services in a competent and workmanlike manner consistent with industry standards (the foregoing clauses (i) and (ii), collectively, the "Cora Warranty"). In the event the Services are not performed as warranted, Customer must notify Cora in writing of the issue with the Services within thirty (30) days providing a description of the deficiency.

c) CORA DOES NOT WARRANT THE SERVICES WILL BE PERFORMED WITHOUT ERROR OR WITHOUT INTERRUPTION, THAT THE SERVICES WILL MEET THE CUSTOMERS EXPECTATIONS OR REQUIREMENTS OR THAT CORA WILL CORRECT ALL ERRORS. CORA SHALL NOT BE RESPONSIBLE FOR DEFICIENCIES OR ISSUES RELATED TO THE OPERATION, PERFORMANCE, OR SECURITY OF THE SERVICES ARISING FROM SERVICES PROVIDED BY THIRD PARTIES OR FROM THE CUSTOMER DATA.

d) IN THE EVENT OF A BREACH OF THE CORA WARRANTY, CUSTOMER'S EXCLUSIVE REMEDY AND CORA'S ENTIRE LIABILITY SHALL BE AT CORA'S OPTION EITHER (i) CORRECTION OF THE DEFICIENCY THAT CAUSED THE BREACH OF WARRANTY, OR (ii) IF THIS IS NOT COMMERCIALLY PRACTICABLE IN CORA'S OPINION, EITHER PARTY MAY END THE DEFICIENT SERVICES, IN WHICH CASE CORA SHALL PROVIDE A REFUND OF PREPAID AND UNUSED FEES FOR THE PERIOD FOLLOWING THE DATE OF TERMINATION.

e) EXCEPT FOR THE EXPRESS WARRANTIES PROVIDED IN THIS CLAUSE 18, TO THE EXTENT PERMITTED BY LAW, CORA EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) FOR SOFTWARE, NETWORKS OR ENVIRONMENTS, SYSTEMS, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, THAT THE SAAS WILL MEET SPECIFIC REQUIREMENTS, MERCHANTABILITY, THAT THE SERVICES WILL BE UNINTERRUPTED, FREE FROM SOFTWARE ERRORS, COMPLETELY SECURE, OR THAT DEFECTS AND DEFICIENCIES IN THE SAAS OR SERVICES WILL BE CORRECTED.

19. Liability

a) NEITHER PARTY SHALL BE LIABLE FOR ANY LOSS OF TURNOVER, LOSS OF SALES, LOSS OF REVENUE, LOSS OF PROFITS (EXCLUDING PAYMENT OF FEES UNDER THIS AGREEMENT) LOSS OF FUTURE REVENUE, LOSS OF GOODWILL, DATA, DATA USE, REPUTATION, OR ANY INDIRECT DAMAGES, CONSEQUENTIAL OR SPECIAL LOSS SUFFERED BY THE OTHER.

b) THE TOTAL AGGREGATE LIABILITY OF CORA AND ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT WHETHER IN CONTRACT, TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED THE FEES PAID TO CORA IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM WILL NOT ENLARGE THIS LIMIT. HOWEVER, THIS LIMITATION SHALL NOT APPLY TO LOSS OR DAMAGE ARISING OUT OF DEATH OR DAMAGE FOR WHICH LIABILITY CANNOT BE LIMITED OR EXCLUDED BY LAW.

20. Indemnity

a) In the event a third party makes a claim against either Cora or Customer (the "Indemnitee" referring to the recipient of allegedly infringing Material) that any software, service, data, hardware, information, design, specification, or material (collectively, "Material") provided by the other party (the "Indemnitor") and used by the Indemnitee infringes the third party's intellectual property rights (a "Third Party Claim"), the Indemnitor shall defend and indemnify the Indemnitee against the Third Party Claim from the damages, liabilities, and costs awarded by the court to the third party claiming infringement or the settlement agreed to by the Indemnitor provided the Indemnitee:

    i. Gives the Indemnitor prompt notice in writing of any Third-Party Claim;

    ii. Give the Indemnitor sole and exclusive right to control the defence and settlement of the Third-Party Claim, and

iii.   Give the Indemnitor all reasonable assistance in the defence of such Third-Party Claim.

b) The foregoing obligations of the Indemnitor shall not apply with respect to a claim of infringement that arises out of (a) any modification or alteration of the Materials other than by the Indemnitor; (b) use of the SaaS in combination with any software, hardware, network, technology or system not supplied by Cora where the alleged infringement relates to such combination, (c) compliance with Customer specifications.

c) If any Third-Party Claim which Indemnitor is obligated to defend has occurred, the Indemnitor may, at its option: (a) obtain for Indemnitee the right to continue using the Materials; (b) replace or modify the Materials so that it avoids such claim; or (c) if such remedies are not reasonably available, terminate the license for the infringing Material and require its prompt return and refund any unused, prepaid fees the Indemnitee may have paid to the other party for such Material.

d) Customer may make a claim in accordance with the above only where Customer provides Cora with written notice of the same no later than sixty calendar days after the party knew, or should have been aware, of the grounds for the claim.

e) This Section 20 constitutes the exclusive remedy the parties' have for any infringement claims or damages.

21.   Supplier Permission

a) The Customer permits Cora to use its name, logo and/or trademark in connection with promotional materials which may be disseminated to the public. These may include, but are not limited to, advertising, social media promotions, press releases, and website use. Cora may distribute a quote from Customer providing testimonial from their project sponsor or spokesperson about their reasons for signing with Cora and hopes for implementation.

b) Following implementation, Customer will cooperate with Cora in creating video interviews with client spokespersons and written case studies. Cora may post such materials on Cora's website, social media, and/or video hosting platforms for promotional purposes.

c) Cora hereby grants Customer permission to use Cora's logo for marketing purposes but only in compliance with Cora's Brand Identity Guidelines, which will be provided to Customer upon request.

22.   Term and Termination

a) The Subscription Term shall commence on Subscription Start Date listed in the Sales Order and, unless terminated earlier in accordance with the terms of this Agreement, shall continue in force for the period set forth in the Sales Order (the "Initial Term"). This Agreement shall renew automatically at the end of the Initial Term for additional successive terms (the "Renewal Term/s") at Cora's then current terms and conditions unless notice is given by either party one hundred eighty (180) days prior to expiration. The Renewal Term is equal in length to the Initial Term unless otherwise stated in the Sales Order.

b) A party (the "Initiating Party") may terminate this Agreement with immediate effect by written notice to the other party (the "Defaulting Party") on or at any time after the occurrence of one or more of the events specified below in relation to the Defaulting Party.

The events are:

i. the Defaulting Party being in material breach of an obligation under this Agreement or any Sales Order or Statement of Work and, if the material breach is capable of remedy, failing to remedy the breach within thirty (30) days starting on the day after receipt of written notice from the Initiating Party giving details of the material breach (for the avoidance of doubt, a "material breach" is any breach that is not capable of remedy and/or is not remedied within thirty (30) days starting on the day after receipt of written notice by the Defaulting Party from the Initiating Party or such further period as may be agreed by the Parties hereto); or

ii. the Defaulting Party fails to make a payment to the Initiating Party of a sum that is properly due to that Party pursuant to this Agreement; or

iii. this Agreement shall terminate immediately if an order is made or an effective resolution is passed or any proceedings are taken for the winding up of either Party or a receiver, manager, examiner or liquidator is appointed over the whole or substantial part of either the Customer or Cora unless both parties agree in writing that this Agreement continues in effect.

c) In the event this Agreement is terminated for cause, all Sales Order and Statements of Works that have been placed under the Agreement shall terminate automatically. Except as provided herein, each party's further rights and obligations cease immediately on termination of this Agreement. Termination of this Agreement shall not prejudice any rights of either party which may have arisen on or before the date of termination. Upon termination Customer shall immediately pay all unpaid sums under any terminated Sales Order or Statements of Work as well as any amounts that have accrued prior to termination and related taxes and expenses.

23. Government Restricted Rights

a) This clause 23(a) applies to all acquisitions of the SaaS by or for the United States federal government, including by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement, or other activity with the Federal Government. The SaaS and related documentation were developed at private expense and are "Commercial Items", as that term is defined at 48 C.F.R. § 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. § 12.212 (for civilian agencies) and 48 C.F.R. § 227.7202 (for Department of Defence agencies), as applicable. Consistent with and subject to 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202-1 through 227.7702-4 as applicable, the Commercial Computer Software and Commercial Computer Software documentation have the potential to be licensed to U.S. Government end users (a) only as Commercial Items and (b) with only such rights as are granted to all other end users pursuant to the terms herein. Any provisions of this Agreement inconsistent with federal procurement regulations or other federal law are not enforceable against the U.S. Government. Unpublished rights are reserved under copyright laws. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in the software or on any packaging or other media associated with the software. This clause 23 does not grant Customer any rights not specifically set forth in this Agreement including without limitation any right to distribute the software to the United States federal government.

b) If Customer is a government entity or is otherwise subject to government procurement requirements, Customer represents and warrants that (1) it has complied and will comply with all applicable government procurement laws and regulations; (2) it is authorized to use the SaaS and enter into this Agreement; and (3) this Agreement satisfies all applicable procurement requirements.

24. Notices

Except for daily contact required between the Parties for the operation of the Agreement and except for as otherwise provided herein, any notice given under this Agreement shall be given in writing and sent to;

For the Customer

the Account Contact listed on the Sales Order.

For Cora:

contracts@corasystems.com

25. Amendment

Cora may amend this Agreement from time to time to reflect changes in, among other things, regulations, laws, technology, and industry practices, provided any changes to the terms will not adversely impact the functionality and security of the SaaS, and will provide notification to Customer thereof. Such an amendment shall be deemed accepted and become effective upon the earlier of thirty (30) days after such notice or Customer's continued use of the Services (the "Proposed Amendment Date"). The Customer may reject the proposed amends, acting reasonably, within 30 days of receiving notice of the amends and in case of such rejection, this Agreement will continue under its original provisions, and the amendment will become effective at the start of Customer's next Renewal Term following the Proposed Amendment Date (unless Customer first terminates this Agreement pursuant to Clause 22 Term & Termination). Customer recognizes and agrees that Cora's online privacy policy is not incorporated into this Agreement, and Cora may revise it at any time in its sole discretion, with or without following the procedure of this clause herein.

26. Force Majeure

a) Neither of the Parties shall be in breach or otherwise be liable to the other party in any manner whatsoever for any failure or delay in performing its obligations under this Agreement (except for delay in the payment of amounts due hereunder and except for as regards maintaining confidentiality) to the extent that it is prevented, hindered or delayed from or in performing such obligations by circumstances beyond a party's control and which could not reasonably have been foreseen. Such force majeure events include inter alia, labour conflicts, lightning, fire, acts of terrorists, war declared or threatened, sabotage or acts of vandalism, natural disasters, decisions of public authorities or other public regulations, errors in another operator's network, general scarcity of transport, goods, or energy, or other similar circumstances. A party must give notice to the other party forthwith (upon becoming aware of the same).

b) In the event a party's performance is delayed for longer than three months due to an event as stated above, either party may terminate the Agreement without penalty.

27. Assignment

a) Neither party may assign this Agreement without the other's written consent, except that Cora may assign this Agreement to its Affiliate which is defined as any partnership, corporation, trust, or any other entity that, directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with a party ("Affiliate") or in connection with an acquisition, merger, re-organization, or sale of its assets or equity.

      i.   Authorized assignment of this Agreement releases and discharges the assignor of all rights, obligations, and liabilities pursuant to this Agreement related to acts and omissions after assignment.

      ii.   No assignment of this Agreement becomes effective unless and until the assignee agrees in writing to be bound by all the assigning party's obligations in this Agreement.

b)   The Customer may assign its Subscription to a third party only with written approval from Cora and at Cora's sole discretion. Cora may require written evidence that the third party accepts the terms and conditions of this Agreement.

28. Governing law and jurisdiction

a)   This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of the Republic of Ireland. The parties hereby submit to the exclusive jurisdiction of the Irish courts in any dispute or claim arising out of or in connection to this Agreement.

b)   The United Nations Convention on the International Sale of Goods shall not apply to this Agreement.

c)   In the event a dispute arises in relation to this Agreement, the parties shall, to the extent it is reasonable under the circumstances, first make good faith efforts to resolve such dispute through negotiation prior to commencing court proceedings.

29. Entire Agreement

a)   This Agreement and materials incorporated by reference herein constitutes the entire agreement between the Parties and supersedes all previous agreements and representations of whatever nature unless expressly incorporated by reference in this Agreement. The Parties disclaim any reliance upon any representations or warranties beyond those set forth in this Agreement including prior discussions, RFP's, and emails. Terms and conditions attached to any customer invoice, purchase order, or other administrative document shall not be deemed to modify, supplement, or add to the terms of this Agreement.

b)   Any terms and conditions contained in the Customer's purchase order are not applicable to this Agreement unless specifically incorporated into this Agreement in writing in advance.

30. Export laws

The Services or components of the Services which Cora may provide or make available to Customer may be subject to U.S. or Irish export control and economic sanctions laws, rules, and regulations. The Customer shall comply with export laws and regulations of applicable jurisdictions in using the Services. Without limiting the foregoing, Customer represents and warrants that a) it is not located in, and shall not use the SaaS from any country subject to United States export restrictions (currently including Cuba, Iran, North Korea, Syria, the region of Crimea, and Sudan); b) Customer shall not use the SaaS in violation of any United States, EU, UK, or Irish, export embargo, prohibition, or restriction; and c) Customer is not prohibited from participating in United States, EU, UK, or Irish export transactions. Without limiting the foregoing, Customer will comply with U.S. Export Administration Regulations and International Traffic in Arms Regulations and sanctions regulations administered by the U.S. Office of Foreign Assets Control ("OFAC") ("Trade Laws"). Customer will not take any action that causes Cora to violate Trade Laws or put it at risk of becoming subject to sanctions and penalties under such laws.

31. General Terms

a) Terms governing confidentiality, liability, intellectual property and any provision that by its nature is intended to survive termination of this Agreement shall survive any termination of this Agreement.

b) If any provision of this Agreement is deemed unenforceable for any reason, the unenforceable provision shall be amended to the extent permitted by law to achieve as nearly as possible the same intent and economic effect as the original provision and the remainder of the Agreement shall continue in full force and effect.

c) There are no third-party beneficiaries to this Agreement.

d) Nothing in this Agreement shall be interpreted as creating any joint venture, partnership, agency, or employment relationship between the parties.

e) The Sales Order, CDPA, and other articles incorporated by reference herein form part of this Agreement.

f) In the case of any conflict between the documentation, the order of precedence shall be as follows:

    a. Cora Data Protection Appendix

    b. Sales Order

    c. Subscription Services Agreement

    d. Statement of Work

g) Cora's failure to enforce any provision of this Agreement will not constitute a waiver. Any waiver of Cora's rights or interests must be in writing and signed by Cora.

32. Definitions

The definitions and rules of interpretation below apply in this Agreement.

"**Business Day(s)"/ "Working Day(s)/" Working Hours""** means Monday to Friday 8.30 am to 6.00 pm GMT excluding the 17th of March, the first Monday in August, the last Monday in October, the 24th and 31st of December and 1st of January.

"**CPI**" or "**Consumer Price Index**" means the Consumer Prices Index as published by the US Bureau of Labor Statistics from time to time, or failing such publication, such other index as the parties may agree most closely resembles such index.

"**Customer**" Means the entity who activates Services provided by Cora and assumes responsibility for payment for the same.

"**Customer Data**" means information and data inputted and stored by Users into the SaaS.

"**Documentation**" means collectively, the Cora Data Processing Appendix, the Security Policy, the Subscription Services Agreement, and any other Cora documents that are incorporated into the Customer's Sales Order.

"**Intellectual Property Rights**" means patents, rights to inventions, copyright and related rights, trademarks, trade names and domain names, rights in get-up, rights in goodwill or to sue for passing off, rights in designs, rights in computer software, database rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights (to include any design, specification, ideas, know-how, techniques, documentation, software, reports that may be developed herein and/or supplied herein), in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewals or extensions of, such rights and all similar or equivalent rights or forms of protection which may now or in the future subsist in any part of the world.

"**Parties**" together the Customer and Cora.

"Professional Services" means any training, configuration, design, project management, business analysist services, consultancy and specialist services procured from Cora by Customer through a Sales Order or Statement of Work.

"RFP" means documents associated with a request for proposal or similar bidding process submission.

"**Sales Order**" Means a Cora pricing document that has been issued by Cora and executed by Customer which indicates the items and/or services to which the customer has subscribed.

"SaaS" means, collectively, the Cora PPM online application and any additional modules to which the Customer has subscribed, and Cora SPM online application and any additional modules to which the Customer has subscribed, each as described in its applicable documentation and as procured by Customer from Cora in the Sales Order, including associated Cora mobile application(s).

"**Services**" means collectively, the Professional Services, Maintenance, Support, and provision of the SaaS.

"**SOW**" means a Statement of Work.

"**Subscription**" means the permission granted by Cora to Customer under this Agreement to use the SaaS.

"**Subscription Start Date**" means the date on which the Services shall be activated and is indicated on the Sales Order.

"**Subscription Term**" means the **Initial Term** and any subsequent **Renewal Term** taken together.

"**Trial**" means access given free of charge to the SaaS or to a version which is under development or evaluation for demo, trial, evaluation, or other similar purposes.

"**User/s**" means individuals who have been authorized by Customer to access or use the SaaS pursuant to this Agreement.

"**Website**" means the Cora Systems website at https://corasystems.com/.

Interpretation

A. The headings in this Agreement are inserted for convenience only and shall not affect its construction. A reference to a particular law is a reference to it as it is in force for the time being taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it.
B. Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.
C. Unless the context otherwise requires, words in the singular include the plural and, in the plural, include the singular.
D. Any words following the terms "including", "include", in particular, or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.
E. This Agreement may be executed in any number of counterparts.

Service Level and Support Objectives

Introduction

1.1 Background

Cora Systems ("Cora") and the Customer have entered into a Subscription Service Agreement (the "SSA") for the Customer to use its current version of the programme and project management software application developed by Cora called "Cora PPM". The terms and conditions in relation to the use of Cora PPM are set out in the SSA and related documents.

1.2 Purpose of Agreements

Under these Service Level and Support Objectives (the "Service Levels") Cora is responsible for providing technical support and maintenance for Cora PPM to the Customer. The type and level of service to be provided is set out herein. The Customer is not permitted to use a third party to provide technical support and maintenance services for Cora PPM. These Service Levels form part of the SSA and should be read in conjunction with that document. Definitions described in these Service Levels have the same meaning attributed to them in the SSA.

1.3 Scope

The scope of this document relates to the standard levels of support afforded to the Customer for the functionality provided by the latest version of Cora PPM. The scope of support relates only to the production sites. It does not relate to implementation, configuration, integration, customization services, training, UAT, non-conformities caused by unauthorized misuse, alteration, modification of Cora PPM, third party applications which may be integrated with Cora PPM, hardware and software not supplied or developed by Cora, or the Customer's use of Cora's API, and use not permitted in the SSA and related documents.

1.4 Duration of Agreement

These Service Levels cover support for the duration of the SSA subject to the fees being paid as set out in the SSA.

1.6 Network Uptime

The application will be available during a 99.9% monthly average scheduled Uptime of the Cora software application during the business hours 08:30-17:00 GMT as measured on a three-month moving average.

This excludes malicious attacks on the services such as DDos (distributed denied of service) or Dos (denial of service), scheduled maintenance and prior notified upgrades of their servers. These upgrades/backups take place outside of core business hours. "Uptime" is defined as your ability, via web browser, to retrieve the application from a hosting server. Application unavailability caused by network unavailability is not included in application Uptime if such network unavailability is caused by force majeure circumstances including problems on the backbone or on the customers portion of the network. Cora will let the Customer know of upgrades carried out by the hosting provider when it is notified of them.

Support Services

2.1 Support Channels

A dedicated, secure helpdesk is established for the Customer at the following address:

https://cst.corasystems.com/support/home

to enable the Customer's users to log support and technical maintenance issues on a 24/7 basis. This helpdesk will be the primary channel for the logging of all support and maintenance issues that arise for the Customer.

Free phone contact details:

Ireland 1800 940940 / UK 0800 043 2078 / US +18332695756/ HQ 00353 719622078

Support will be available:

Monday - Friday from 08:30 - 17:00 GMT on a Business Day.

Cora provides 24x7x365 resourced support for Severity 1 and Severity 2 issues that have been raised via our Helpdesk that may occur outside of standard Cora support hours.

2.2 Service Level Agreements

Cora Support Matrix:

Security Level	Description	Initial Response Time	Target Resolution
1	Access is denied to all users or major loss of business capability	Immediate	100% < 4 Working Hours
2	Site access denied to a group of users	<60 mins during Working Hours	98% < 1 Business Day
3	Site access denied for single user	<60 mins during Working Hours	98% < 2 Business Days
4	Loss of minor business capability	<60 mins during Working Hours	100% < 3 Business Days
5	Minor issue with Application functionality	60% < 0.5 days 85% < 1 day 98% < 2 days	100% by next revision if applicable

Each call received by the support staff will receive a severity level based on the table above. Escalation of a call will be by the team leader, based upon the customer feedback and timeframe. It is a goal of the support staff to have all problems resolved within two working days. Support staff will endeavour to resolve the highest severity issues within working or non-working hours. No problem will be left unassigned for more than 60 minutes during working hours. The fix for minor bugs and issues may be included in the next revision of the software and will berolled out in the next upgrade so therefore may not be addressed until

the next upgrade or version. Support call performance reports will be generated upon request from the customer.

2.3 The Cora Support Helpdesk

Ticket Status:

Once logged on the Cora Support Helpdesk, tickets will be assigned the following status types:

Status	Description	SLA Active
Open	New Ticket Logged on Helpdesk.	Yes
Under Investigation	Ticket has been assigned to a member of the CCST team and is currently under investigation.	Yes
With Third Party	A resolution for the issue is dependent on input from a Third party or external supplier.	Yes
Change Request*	A change to Cora PPM has been identified as a result of the issue being raised and the issue is marked as a change request. As such the issue will be put through a change control process where it will be analysed, estimated, scheduled and approved for release in a future iteration of Cora Software.	No
Bug Identified	The issue has been reproduced by CST and has been confirmed as a Bug.	Yes
Bug Fix Scheduled	The Issue has been scheduled for fixing by the Cora R+D Team.	Yes
Bug Fixed, awaiting scheduled upgrade	The Issue has been fixed and tested by Cora, and Cora await agreement with the Customer to put the fix (or new build) on to the Customer's UAT site for verification purposes.	Suspended
Unable to complete Upgrade	Cora are unable to complete an upgrade containing a fix for the issue due to remote access difficulties.	Suspended
Duplicate Ticket	This ticket is a duplicate of one already logged on the helpdesk.	No
Awaiting Approval to Upgrade Live	A fix has been applied to the UAT site and confirmed by the Customer. Cora await final approval from the Customer to upgrade the live site with the new build or fix.	No
Closed	Issue has been confirmed as resolved by the Customer and can now be closed off.	No

*Change Requests are dealt with using the change request process set out in the SSA and may incur additional charges.

Upgrades

3.1 Upgrade Process

The Customer will be entitled to receive upgrades at no additional cost provided all payments due have been paid in full. There are typically 2-4 upgrade releases per year. Each upgrade is supported with supplementary release notes.

The standard support policy is to maintain the Customer on the most recently upgraded version of the software as all product fixes and enhancements will be contained in the most recent release. These Service Levels do not apply where the Customer is more than two versions behind the latest version.

Additional services, which may be required by the Customer as part of the upgrade process, are as follows below and are provided on a chargeable basis, with costs to be agreed with the Customer:

- Business consulting on new features, best practice and training
- Technical consulting on integration and other custom software, impact analysis and upgrade
- Assistance with user acceptance regression testing of modifications or enhancements to the software
- Project Management expertise to assist with upgrades
- Product enhancement for new features to be included with the upgrade

3.3 Upgrade Timeframe

Cora will endeavour to complete an upgrade within 1 Business Day. However, where unforeseen technical difficulties occur, an upgrade may take longer depending on the issues. Cora will communicate any issues arising with the Customer through the communication channels outlined in this document.

3.5 Access

As this is a hosted solution Cora will arrange and manage the remote access requirements to the hosting centre and servers. Cora will require access to the application site and the database of the Customer UAT and Live sites as part of the support process (e.g., to aid issue reproduction/ debugging). Cora may access the UAT and Live sites for the purposes data and usage analysis in order improve its product and services. None of the data will be retained or used by Cora in a way that breaches its confidentiality requirements. Cora will keep a log of any access to the database with the measures, who accessed, when and why.

3.6 Data

In advance of the termination of the SSA, the Customer should remove any data from Cora PPM that it requires. The report suite in Cora PPM provides for the extraction of data from the system. Following termination, Cora will delete the Customer's environment and any data therein in accordance with Cora's Customer Deletion Procedure. Where the Customer requires technical assistance to extract their data this will be deemed outside of the scope of this SSA and all such work will be pre-agreed and charged on a time and materials basis.

3.7 Emergency Support

The Customer will endeavour to provide support outside of Working Hours however it cannot guarantee the availability of emergency support staff and the resolution of any items outside of Working Hours.

Backup and Recovery

Cora will operate a standard backup and recovery process. The database will be backed up on a daily basis, outside Working Hours and stored in a remote location. The backup schedule is as follows:

- Daily backups will be retained for a rolling 28 days period.
- Monthly backups will be retained for a period of 3 months, with the monthly backup being taken on the 1st of each month.

In the event of a loss of service for an extended period (>4 hours) Cora will put into effect the recovery plan whereas the Site will be restored to a new server, within one Working Day, with the last backup available. This will be done in consultation with the Customer and reasonable efforts will be made to keep them informed at all times through the agreed communication channels.

3.8 Recovery Point Objectives (RPOs)

RPO focuses on data and Cora's resilience to the loss of it in a disaster. Standard RPO for Cora PPM is 24 hours – accomplished through nightly backups across a fully managed and monitored backup solution. RPO for designated Live databases will be 1 hour. Live databases can be restored quickly from the previous 28 days and Day 1 of the previous 3 months.

3.9 Recovery Time Objectives (RTOs)

RTO looks at the whole business and systems involved, and is the target time set for the recovery of IT and business activities after a disaster has struck. Standard RTO for Cora PPM is 48 hours. Current virtual infrastructure redundancies help reduce the risk of a major disaster. Cora endeavours to restore any interruption in service at the earliest possible time.

Cora Data Protection Appendix

The parties agree that this Cora Data Protection Appendix (the "**CDPA**") sets forth their obligations with respect to the Processing of Personal Data in connection with the performance of the Subscription Services Agreement ("**SSA**"). This CDPA forms an integral part of the SSA and is effective upon execution of a Sales Order. In case of any conflict, this CDPA will have precedence over the terms of the SSA to the extent of such conflict.

Definitions

"**Applicable Data Protection Law**" means all data protection laws that apply to the Processing Personal Data under this CDPA.

"**Breach**" means a breach of physical or digital security that results in accidental or unlawful destruction, loss, alteration, or disclosure of, or access to, the Personal Data. Unsuccessful attempts or activities that do not compromise the security of Personal Data shall not be considered a Breach, including failed log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Cora**" Means the Cora Systems Affiliate that has executed the SSA.

"**California Personal Data**" Means Personal Data that is subject to the CCPA.

"**CCPA**" means the California Consumer Privacy Act of 2018 (California Civil Code Sec. 1798.100).

"**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.

"**Data Protection Requirements**" means European Data Protection Laws, and any applicable laws regulations, and other legal requirements relating to privacy, data security, and the use, collection, storage, retention, disclosure, transfer, and processing of Personal Data.

"**Data Subject**" means an identified or identifiable natural person.

"**European Data Protection Laws**" means data laws applicable in the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom. This includes (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) UK Data Protection Act 2018 ("**UK DPA**"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("**Swiss DPA**"); in each case, as may be amended, superseded or replaced.

"**European Data**" means Personal Data that is subject to the GDPR.

"**Instructions**" means the written instructions issued by a Controller to a Processor to direct such Processor to perform a specific or general action with respect to Personal Data. The processing activities contemplated in the Agreement and CDPA constitute Instructions,

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

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"**Process**" or "**Processing**" is as defined in the Applicable Data Protection Law.

"**Sensitive Personal Data**" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"**Standard Contractual Clauses**" means those clauses in the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of data to third countries pursuant to Regulation (EU) 2016/679.

All other capitalized but undefined terms shall have the definitions given them in the SSA.

1 Scope

a)   This CDPA applies to Cora's Processing of Personal Data on behalf of Customer to provide the Services as set forth in the SSA.

b)   The parties acknowledge Customer is the Controller and Cora is the Processor with respect to the Services.

2 Responsibilities of the Parties

a)   Cora shall only process Personal Data in accordance with Instructions from Customer.

b)   Both parties shall, where applicable, comply with transparency and lawfulness requirements under applicable data protection laws including with respect to the rights of Data Subjects.

c)   Customer is responsible for the accuracy, quality and lawfulness of the Customer Data.

d)   In particular, Customer shall ensure any Personal Data has been lawfully collected under an appropriate legal basis and may lawfully be provided to Cora in accordance with the terms of the SSA and this CPDA.

e)   The parties do not contemplate the Processing of Sensitive Personal Data or special categories of Personal Data. Unless otherwise provided in the SSA or Sales Order, Customer may not provide Sensitive Personal Data to Cora.

f)   Customer is responsible for determining whether the security measures provided for the Services meet Customer's obligations under Applicable Data Protection Laws including with respect to the security of data while in transit to and from the SaaS.

g)   Customer recognizes Cora's mobile and web applications are freely accessible to Customer's Users and control over locations from which the app may be accessed lies with the Customer and not with Cora. Customer shall be responsible for authorization and management of User accounts across geographies including with respect to the transfer of Personal Data.

3 Controller Instructions:

a) The parties agree that the Customer's complete Instructions to Cora in relation to the Processing of Personal Data includes the SSA together with Customer's use of the Services in accordance with the SSA.

b) Customer may provide additional reasonable written Instructions during the Subscription Term with respect to the Processing in accordance with Applicable Data Protection Law and Cora shall comply with such instructions to the extent necessary for Cora to (i) comply with its obligations as a Processor or (ii) to assist Customer to comply with its obligations under Applicable Data Protection Law in relation to Customer's use of the Services.

c) As between the Parties, Cora shall have no liability arising from Cora's compliance with instructions received from Customer. However, Cora shall notify Customer where it believes it has received Instructions that are unlawful or beyond the scope of Cora's obligations in operating the Services or providing Professional Services to Customer. The parties acknowledge that Cora is reliant upon Customer's representations regarding the extent to which Cora is entitled to Process the Personal Data.

d) If Cora receives Instructions to Process Personal Data in a way that goes beyond what is covered by the fees for the Services as described in the SSA, Cora shall notify Customer of any additional fees Cora expects to incur in complying with such Instructions and the parties shall negotiate in good faith with respect to any such charges or fees.

4 Confidentiality

Cora shall ensure that persons Cora authorizes to process the Personal Data are under appropriate confidentiality obligations in relation to the Personal Data.

5 Security

Cora shall implement and maintain appropriate technical and organisational safeguards to prevent the accidental or unlawful destruction, loss, alteration, or disclosure of the Personal Data as described in the Security Policy which includes further details on Cora's security measures in relation to the Services specified in the Sales Order. Such measures are designed to maintain the security, confidentiality, and integrity of Customer Data and include physical access controls, redundancy, data separation, and risk assessment and management processes. Notwithstanding any provision to the contrary, Cora may modify or update the Security Policy at Cora's discretion provided such update does not result in a material degradation in protection.

6 Subprocessors

a) Customer confirms Cora has general permission to utilize Sub-Processors to Process Personal Data. Cora's Sub-Processors are listed in the Customer Portal and Cora shall notify Customer prior to engaging any additional Sub-Processors where such notice is required by law.

b) Cora shall impose contractual data protection obligations on Sub-Processors that provide at least the same level of protection for Personal Data as does this CDPA. Where appropriate, this shall include Standard Contractual Clauses.

c) Cora shall be responsible for the acts and omissions of each Sub-Processor in relation to such Sub-Processors commitments under Applicable Data Protection Law and in relation to compliance with the commitments in this CDPA.

7 Privacy requests from individuals

a) Customer may address privacy requests received from individuals by utilizing the SaaS functionality or, to the extent such access is not available, Customer may seek assistance from Cora by submitting a support request as outlined in the Service Level and Support Objectives (the "Service Levels") with detailed instructions on how Cora may fulfil such request.

b) If Cora receives requests from individuals for which Customer is the Controller, it shall pass on such requests to Customer whereupon Customer shall become responsible for responding to such request.

c) The parties acknowledge Customer is solely responsible for carrying out its obligations as a Controller. Where applicable, Cora will assist Customer in complying with Customer's obligations as a Controller pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of Processing, by providing information required to conduct Data Protection Impact Assessments or responding to Data Subject access requests. The foregoing is subject to Clause 3d (Controller Instructions).

8 Deletion or Return of Personal Data

Upon termination or expiration of the SSA, Cora shall return, including by providing available data retrieval functionality, or delete any remaining copies of the Customer Data (including Personal Data) Processed under this CDPA in accordance with the procedures set out in the Service Levels. This Clause 8 shall apply except to the extent Cora is required by applicable law to retain data, records, or information.

9 Audits

a) Cora will, upon reasonable request and to a maximum of once per year, provide Customer with sufficient information to enable the Customer to ensure Cora complies with its obligations under this CDPA.

b) Subject to Clause 9d, Customer may itself audit Cora's compliance with its commitments under this CDPA once per year. Additionally, to the extent required by Applicable Data Protection Law, Customer or a competent regulatory authority may perform more frequent audits.

c) Subject to Clause 9b and Clause 9d, Customer may, at its own cost, appoint an independent auditor for the purposes of exercising its rights under this Clause 9 (Audits) subject to Cora's reasonable written agreement to Customer's choice of third-party auditor.

d) For any audit Customer wishes to perform whether itself or through a third party, Customer shall;

    a. Submit an audit plan to Cora two weeks in advance of the proposed audit date describing the scope, duration, and date of the audit.

    b. Cora shall review such plan, notify Customer if it has any questions or concerns, and cooperate with Customer to agree on a final audit plan.

    c. Compensate Cora for reasonable costs Cora incurs as a result of the audit.

e) Any audit shall be conducted during regular business hours.

f) Any auditor shall be under appropriate contractual or statutory confidentiality obligations and all information relating to such audit shall be subject to the Confidentiality provisions of the SSA. Audit reports may only be used to confirm Cora's compliance with the requirements of this CDPA or meeting Customer's own regulatory audit requirements. Cora shall have the right to review audit reports and to issue a reply prior to issuance of a final version. The Customer shall ensure the requirements of this Clause 9f are present in Customer's contract with any third-party auditor.

10 Data Transfers

a) Customer acknowledges and agrees that, without prejudice to any applicable restrictions specified in Customer's Sales Order or the Agreement, Cora may Process Personal Data globally as necessary to perform the Services. Personal data may be transferred to Cora Systems US Inc. in the United States and jurisdictions where Cora's Subprocessors and affiliates operate.

b) To the extent such global processing involves the transfer of Personal Data which is subject to regulation and restriction on cross-border transfers under Applicable Data Protection Law, Cora shall put appropriate safeguards in place in accordance with applicable law including Standard Contractual Clauses where necessary.

11 Breach notices

Cora will notify Customer without undue delay after becoming aware of a data Breach that may put the confidentiality or security of the Personal Data in jeopardy. In such an event, Cora will collaborate with Customer and fulfil any reasonable requests by Customer for updates so long as such requests do not interfere with Cora's investigation and mitigation of the effects of the breach.

12 Compliance Requirements

If Cora is required by law to provide access to Personal Data such as in compliance with a subpoena, court order, or other government requests, Cora will inform Customer of such a request to the extent such notice is reasonably practicable and permitted by law.

13 Data Protection Contact

Data Protection queries and communications may be submitted to the Cora privacy team at: info@corasystems.com

14 Additional European Data provisions

This Clause 14 shall apply only with respect to Cora's Processing of European Data in providing the Services.

a) Customer may provide Instructions to Cora with respect to data transfers, assistance with Data Subject requests to delete, erase, access, restrict, rectify, transmit, block access to, or object to the Personal Data Processing.

b) Cora will inform Customer in the event it believes Customer has provided unlawful Instructions.

c)   Subject to the terms and conditions in this CDPA, the SSA, and the Sales Order, Customer grants Cora general permission to engage Subprocessors in the performance of the Services. These Subprocessors are identified in the customer portal.

d)   Cora shall provide Customer notice prior to changing Subprocessors through the following procedure. Cora shall post an amended list of Subprocessors to the customer portal listing the additional replacement Subprocessor and send Customer email notice of the same (the "Subprocessor Change"). Such Subprocessor Change shall be deemed accepted by Customer 30 days after such notice unless Customer first gives Cora written notice of an objection to such change. Such objection shall provide justifiable grounds for the objection relating to the ability of the new Subprocessor to adequately protect Personal Data in accordance with this CDPA or Applicable Data Protection Law. In this event, the parties shall negotiate in good faith to find a mutually acceptable resolution. In the event Cora determines in its sole discretion that a resolution cannot be reached, (i) Customer may terminate the relevant services upon serving 30 days prior notice, and (ii) Cora may at its option terminate the Services immediately. In the event of early termination under this Clause, neither party shall have any liability to the other except that Customer shall not be relieved from payment obligations under the SSA for fees accrued up to the date of termination. If the termination under this Clause relates to part and not to the whole of the Services under a Sales Order, then Customer shall enter into a replacement Sales Order to reflect such partial termination.

e)   Cora will provide reasonable assistance to Customer with any data protection impact assessments (DPIA's) and prior consultations with competent data privacy authorities to the extent required by European Data Protection Laws.

f)   Customer may include the contact details of Customer's Data Protection Officer in their Sales Order.

g)   Further details of Processing of European Data can be found in Appendix 1.

15 Additional Provisions for California Personal Data

This Clause 15 (Additional Provisions for California Personal Data) shall apply only with respect to California Personal Data.

a)   When processing California Personal Data in accordance with your Instructions, the parties agree that Customer is a Business and Cora is a Service Provider for the purposes of the CCPA ("Business" and "Service Provider" are as defined in the CCPA).

b)   The parties agree that Cora will Process the California Personal Data as a Service Provider for the purpose of performing the Services under the SSA or as otherwise permitted by the CCPA.

16 General Terms

a)   The term of this CDPA shall be the Subscription Term of the SSA.

b)   Notwithstanding anything else to the contrary in the SSA, Cora reserves the right to update and amend this CDPA and the SSA Clause 26 (Amendment) shall apply.

c) If any provision of this Agreement is deemed unenforceable for any reason, the unenforceable provision shall be amended to the extent permitted by law to achieve as nearly as possible the same intent and economic effect as the original provision and the remainder of the Agreement shall continue in full force and effect.

d) The liability of each party, taken in the aggregate, arising out of or related to this CDPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in Clause 20 (Liability) in the SSA and any reference in such section to the liability of a party means the aggregate liability of that party under the Agreement (including this CDPA). In no event shall this clause be interpreted to limit either party's liability with respect to any individual's data protection rights under this CDPA or otherwise.

e) This CDPA shall be governed by and construed in accordance with the laws of the Republic of Ireland unless required otherwise by applicable data protection laws.

f) Prior Versions: For earlier versions of this CDPA, please contact info@corasystems.com.

Appendix 1

Details of Processing

Subject matter	Personal Data is processed for the purpose of providing Project Portfolio Management product and services for the Controller to use for planning, maintaining and managing projects.
Duration of Processing Activities	Processing shall occur during the Subscription Term of the SSA and for 30 days thereafter.
Nature and Purpose of the Processing Activities	Cora may Process Personal Information as necessary to perform the Services, including storage, backup and disaster recovery; providing technical support and processing change orders; updating the system and applying new system versions, patches, and upgrades; monitoring and testing system use and performance; performing incident management, maintenance, configuration, IT infrastructure maintenance and troubleshooting, migration, implementation, and performance testing of the system.
Types of Personal Data	Types of Personal Data may include First name, surname, email address, username.
Categories of Data Subject	Categories may include staff, employees, personnel, contractors, suppliers, end users.
Additional Information	Where requested, additional or more specific Processing descriptions may be set out in the SSA.

Security Policy

This Security Policy sets forth administrative, technical and physical safeguards Cora Systems ("Cora") takes to protect customer data. Cora may update this Security Policy from time to time to reflect changes and improvements to our processes and technologies, as well as in response to emerging security threats.

Capitalized but undefined terms shall have the definitions given them in the Subscription Services Agreement ("SSA").

The Framework

Cora has adopted a security model designed to comply with the following international best practice standards; ISO27001/ISO27002, SOC 2 Type 2, Cyber Essentials, and Cyber Essentials Plus.

The following are Cora's key security objectives:

- Ensure that all data is held in a confidential state and only accessible to authorised users.

- Ensure that data integrity is maintained at all times.

- Ensure that data is available to the user when required.

Policies

Cora maintains security policies that are documented, approved, and reviewed by management annually.

Risk Management

Cora has adopted a security model in line with SOC 2 Type 2. A systematic approach to information security risk management is necessary for Cora to identify the business needs to capture and manage information risk in order to meet contractual and regulatory requirements. In order to effectively manage information security risks, we have defined this methodology to reliably undertake repeated risk assessments, allowing Cora Management to identify and prioritise risks to be addressed.

Certifications

Cora security policies cover the management of security for both Cora internal operations and the services Cora provides to its customers, and apply to all Cora personnel, such as employees and contractors. These policies are aligned with SOC 2 Type 2 (or equivalent standards), and guide all areas of security within Cora.

Physical, Technical and Environmental Access Controls

Physical Access Measures

Cora limits physical access to its information systems and facilities to Cora IT Support personnel using physical controls. These shall include a combination of any of the following: CCTV systems, alarm systems, magna locks, pressure sensitive doors, access cards, biometric controls, on-site guards, intruder detection systems, sign in/out procedures, visitor escorting, log review processes. The Cora security team ensures their business partners, in the provision of Cora SaaS software solution also have adequate physical security infrastructure in place (e.g., access cards, biometric access controls, manned data centre security, intruder detection systems, sign in/out procedures, visitor escorting, CCTV, and log review processes in place)

In addition, Cora applies air temperature and humidity controls for its Communications room and protects against loss due to power failure.

Logical Access Controls

Protecting access to IT systems and applications is critical to maintain the integrity of Cora technology and data and prevent unauthorised access to such resources.

Access to Cora IT infrastructure is restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

Cora employs monitoring and logging technology to help detect and prevent unauthorized access attempts to its networks and production systems.

All internal Cora systems require the use of MFA for staff to access.

Access to Cora SaaS software offerings, is protected by authentication and authorisation mechanisms. SAML and Two factor authentication. User authentication is required to gain access to all software offerings. Individuals are assigned a unique user account which is role based and requires a licence to login to the application. Individual user accounts shall not be shared. Access privileges are based on job requirements using the principle of least privilege access.

Threat and Vulnerability Management

Cora utilises a number of network monitoring tools to ensure integrity and performance on our network.

These include tools for security event monitoring, network data monitoring, asset vulnerability scanning and misconfiguration detection.

Malware Protection

Cora uses industry standard endpoint security tools to protect our assets. This cloud managed system ensures our assets can always be contacted regardless of which network they are on and includes endpoint detection and response (EDR) capabilities, vulnerability and patch management, and isolated sandboxing to carry out enhanced analysis of potential malicious processes. This EDR system gives the security team a clear view of all interactions carried out by a user or system giving enhanced visibility across the estate.

External Devices

Cora operates a ban on external devices such as USB keys for the transfer of information.

Firewall

An industry standard firewall is installed and managed to protect Cora. Firewalls are set up to filter unauthorized inbound traffic from the Internet and are configured to deny inbound network connections that are not explicitly authorized by a rule.

Data Segregation

Cora maintains separate environments for production and non-production systems.

Each customer gets:

1) Dedicated infrastructure for that customer.

2) Dedicated and unique IP address and DNS entry.

3) IP Restrictions and whitelisting can be deployed.

These Data Segregation commitments do not apply to customers who are hosting the software on their own infrastructure.

Backups

Cora has a long-standing partnership with our backup solutions provider. Data is automatically compressed, encrypted, and securely transmitted via the Internet to an offsite data centre. Data is also mirrored to a secondary data centre to provide a protective layer of redundancy. Our backup partner, utilises 256-bit SSL encryption which safely secures data during transport over the Internet. Backups also have 256-bit AES encryption which safely secures data on the backup providers servers.

Change Control

Cora change control policy ensures the effective management of change while reducing risk. Key components to the company's Change Management program include:

- Accurate Documentation
- Continuous Oversight
- Scope definition
- Formal, Defined Approval Process

Encryption

Cora utilises industry standard encryption to encrypt customer data at rest and customer data in transit. The customer gets end to end encryption of their data using secure a Https connection using TLS 1.2 cryptographic protocols and are encrypted using SSL certificate with RSA2048 (SHA256withRSA) bit encryption. All data at rest is encrypted using mainstream drive encryption which provides protection for Cora infrastructure as well as the data stored on it.

Penetration Testing

Cora will initiate an annual penetration testing exercise to ensure the processes and procedures in place are robust in stopping attacks and responding quickly and effectively to scenarios. This annual penetration test is performed by a third party. The resulting Executive summary report can be provided to the customer upon request.

Cora customers may request to perform their own Penetration test on the Cora software offerings, at their own expense and only once per year. Facilitating customer requested Penetration tests may incur a fee.

Workstation security

Cora implements and maintains security mechanisms on employee laptops, including Firewalls, anti-virus, and full disk encryption using mainstream drive encryption. Cora operates a least privilege access policy.

Secure Code Review

Cora performs a combination of static and dynamic testing of code prior to the release of code to customers. Vulnerabilities are addressed in a timely manner. Software patches and new releases are regularly made available to customers to address known vulnerabilities and these are subject to quality review prior to release.

Illicit Code

Cora will implement and maintain commercially reasonable measures to prevent the introduction into the subscription service offering of any viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of Cora software offerings; or (b) any interruption, interference with the operation of the Cora software offerings. If Cora software offerings are found to contain any Illicit Code that adversely affects the performance of Cora software offerings or causes a material security risk to customer Data, Cora shall, as customer's exclusive remedy, use commercially reasonable efforts to remove the Illicit Code or to advise and assist customer to remove such Illicit Code. Cora is not responsible for Illicit Code introduced by customer, a third party, or sources other than Cora.

Company Security Measures

Asset Control

Cora records not only the type of software installed on each system, but also its version number and patch level. These details are tracked using an asset management tool. This tool allows Cora IT administrators to monitor all changes in software, hardware, licences and device allocation.

Email Management

Cora uses mainstream subscription services to manage our emails. Security and Compliance scans are employed for all emails that enter and exit a mailbox.

Personnel Security

Employees are subject to background checking, security screening, employment and education verification processes as part of the terms of their employment with Cora.

Security awareness and Data Protection Training

Security Awareness training and Data Protection Training is a requirement for all Cora employees at the time of hire and refresher training is carried out annually. Phishing email awareness training, cyber security awareness training and invoice misdirection training are all carried out.

Vendor risk management

Cora conduct vendor risk management assessments of its hosting and backup solutions providers annually.

Business and Service Continuity

Disaster recovery

Cora has both a Service continuity plan and a Disaster Recovery and Business Continuity Plan. The purpose of the Disaster Recovery Plan maintained by Cora is to outline Cora's' response in the event of a disaster occurring at Cora offices or their environs.

Service Continuity

The service continuity plan is engaged in the event of a disruption of service of our software offering to our customers.

Monitoring and Incident Management

Incident Management

Cora operates and maintains an Incident management policy. Cora will monitor, manage and respond to incidents in a timely manner, tracked via the Cora helpdesk and in line with current Service Levels.

Data breach

Cora operates a data breach process in line with the General Data Protection Regulation as described in the Cora Data Processing Appendix. Cora will contact the customer regarding any accidental, loss or destruction of, alteration, unauthorised disclosure or access to customer data in a timely manner, following determination by Cora that a data breach has occurred.

Cookies

Cora cookie policy is outlined in the below link and may be updated from time to time.

https://corasystems.com/cookie-preferences/

Limitations

Notwithstanding anything to the contrary in this Security Policy or other parts of the SSA, Cora obligations herein are only applicable to the Services as defined in the Subscription Service Agreement. This Security Policy does not apply to: (a) information shared with Cora that is not Customer Data; (b) data in customer's VPN or a third-party network; and (c) any data processed by customer or its users in violation of the Agreement or this Security Policy.