Support Revolution

Third Party Support Services Agreement

This Third Party Support Services Agreement ("Agreement") is made and entered into as of 12/17/2024 (the "Agreement Date") by and between Support Revolution, Inc., a Delaware corporation, whose office is at Support Revolution Inc., 111 Congress, Suite 500, Austin, Texas (the "Supplier") and the County of Fresno, political subdivision of the State of California ("County").(the "Client").

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, the following words and expressions have the meaning set opposite:

"Confidential Information" means: (i) all confidential, technical, scientific, or commercial information (in any form or medium and including all copies of the same) concerning past, present, and/or future transactions, dealings, projects, plans, proposals (including the Proposal), staff and other business affairs that are disclosed directly or indirectly by one party (the **"disclosing party"**) to the other (the **"receiving party"**) at any time in contemplation of or in connection with the Agreement (whether or not it is stated to be confidential at the time of disclosure); and (ii) the terms of the Agreement, in respect of which the Client shall be the receiving party;

"Control" means the ownership of more than 50% of the issued share capital or other equity interest or the legal power to direct or cause the direction of the general management and policies of an entity;

"Customization" means any improvement to, or modification, customization or extension of, the functionality or performance of any Supported Software, other than a Fix;

"Fix" means the correction of an Incident by the Supplier, including the provision to the Client of any patches or documentation that are required for or as a result of such correction;

"Incident" means any defect or error in the Supported Software, including any failure by the Supported Software to perform in accordance with the specifications provided to the Client in respect of such Supported Software;

"Intellectual Property Rights" means patents, rights to inventions, copyright and related rights, trade marks, trade names and domain names, rights in designs, rights in computer software, database rights, rights in confidential information (including know-how) and any other intellectual property rights, 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 subsist or will subsist now or in the future in any part of the world;

"Laws" means any applicable: (a) statute, delegated or subordinate legislation; (b) binding judgment of a court of competent jurisdiction; (c) industry code, standard or policy enforceable by law; and (d) relevant binding regulatory direction, policy or rule, in each case in force at any time during the Term in any jurisdiction applicable to the Agreement;

"Losses" means all claims, actions, proceedings, losses, liabilities, damages, costs, and expenses howsoever arising (including legal fees and other professional advisors' fees, and disbursements and costs of investigation, litigation, settlement, judgment, interest, penalties and remedial actions);

"Patches" means updates to the Supported Software;

"Personnel" means, in relation to a party or a Support Partner, as applicable, that party's employees, agents, consultants and subcontractors who are involved in the performance of the Agreement;

"Proposal" means the Supplier's final signed proposal for the provision of the Services, as provided to the Client;

"Services" means the third party software support services, and (if applicable) any transition services and Trend Micro, to be provided by the Supplier to the Client under the Agreement, as more particularly described in the Proposal;

"Service Levels" means the service levels described in the Service Level Agreement;

"Service Level Agreement" means the Supplier's standard service level agreement in force from time to time;

"Similar Services" means any services that are the same as or similar to the Services to be provided under this Agreement, and/or the performance of any other obligation or activity that is the same as or similar to the obligations and/or activities to be performed by the Supplier under this Agreement;

"Support Partner" means any third party provider of support services to the Client in relation to the Systems and/or the Supported Software;

"Systems" means the Client's IT systems that incorporate the Supported Software, excluding the Supported Software itself;

"Supported Software" has the meaning ascribed to it in Section 6.1.

"Term" means the Initial Term and any Subsequent Terms; and

"Third Party Licensor" means the third party licensor or vendor of the Supported Software.

1.2 In the Agreement, except where otherwise stated or where the context otherwise requires:

1.2.1 Section headings are included for convenience only and will not affect the construction or interpretation of the Agreement;

1.2.2 any phrase introduced by the words **"including"**, **"includes"**, **"in particular"** or similar shall not limit the generality of any preceding words;

1.2.3 any reference to a Section is to the relevant Section of the Agreement;

1.2.4 use of the singular includes the plural and vice versa;

1.2.5 any reference to **"persons"** includes natural persons, firms, partnerships, bodies corporate, corporations, associations, organisations, governments, government bodies, states, foundations and trusts (in each case whether or not incorporated and whether or not having separate legal personality);

1.2.6 the words **"in writing"** and **"written"** exclude fax and email (unless stated otherwise in the Agreement);

1.2.7 the words **"day"** and **"month"** mean calendar day and calendar month;

1.2.8 any reference to a statute or provision of a statute includes references to:

(a) that statute or provision as amended, extended or applied by any other provision regardless of whether the other provision became law before or after the Agreement;

(b) any re-enactment of that statute or provision (with or without change); and

(c) any regulation, order, code of practice or similar thing having the force of law made (before or after the Agreement) under that statute or provision or any provision falling within Sections (1.2.8(a) or 1.2.8(b));

1.2.9 references to **"indemnifying"** any person against or with respect to any circumstance shall include indemnifying and keeping it harmless, on an after tax basis, from all Losses suffered, made or incurred by it arising from or in relation to such circumstance; and

1.2.10 a reference to **"good faith"** in the Agreement means that the applicable party or parties must:

(a) not act unconscionably, use misleading or deceptive conduct nor any element of duress (including economic duress or threat of enforcing legal rights);

(b) act honestly, providing where relevant honest and objective appraisals of any facts or circumstances;

(c) meet with and openly discuss issues where relevant, giving due and proper consideration to the views and needs of the other party as against their own views and needs, all in a professional and responsible manner,

and for the avoidance of doubt, **"good faith"** does not mean a party is obliged to act contrary to its own interests.

2. CONTRACT STRUCTURE

2.1 The Client and the Supplier agree to be bound by:

2.1.1 these terms and conditions (subject to Section 3.3);

2.1.2 the Proposal;

2.1.3 the Service Description; and

2.1.4 the Quotation,

(together, the **"Agreement"**).

2.2 If there is any conflict or ambiguity between the terms of the documents listed in Section 2.1, a term contained in a document higher in the list shall have priority over one contained in a document lower in the list.

3. TERM

3.1 This Agreement shall come into force on the date of this Agreement (the **"Agreement Date"**) and the Supplier shall commence the provision of the Support Services from December 17, 2024 (the **"Support Commencement Date"**). The Agreement will continue for 36 Months (3 Years) from the Support Commencement Date (the **"Initial Term"**) unless it is terminated earlier in accordance with its terms.

3.2 Subject to Section 3.3, at the end of the Initial Term this Agreement may be extended for no more than two one-year periods (each a “Subsequent Term”), upon written confirmation from both parties at least 90 days prior to the end of the Initial Term or the relevant Subsequent Term. The Director of Internal Services/Chief Information Officer, or their designee, is authorized to sign the written approval on behalf of County. The extension of this Agreement by the County is not a waiver of any default or breath of this Agreement by the Supplier existing at the time of the extension whether or not known to the County.

3.3 Before the start of any Subsequent Term: (a) the Supplier may require the Client to agree to the Supplier's most up to date terms and conditions (in which case they shall apply from the start of such Subsequent Term); and/or (b) the parties may review the Supported Software and agree any other changes to the scope of the Services for the relevant Subsequent Term, in which case the Supplier may adjust the Charges accordingly for any Subsequent Terms.

4. CONTRACT MANAGEMENT

4.1 The Client and the Supplier shall each appoint an individual who will serve as the principal interface between the parties with respect to all issues relating to the Agreement (such individual for the Client being the **"Client Representative"** and for the Supplier being the **"Account Manager"**). The Account Manager shall also be responsible for the co-ordination of all matters relating to the Services. Each party may replace such individual from time to time on written notice to the other party.

5. SUPPLY OF THE SERVICES

5.1 The Client appoints the Supplier to provide, and the Supplier shall provide, the Services in accordance with the terms of this Agreement as detailed in Exhibit A titled “Independent PeopleSoft Support Service Description,”, in Exhibit B titled “Amendment to Third Party Support Services”, and any subsequent service descriptions

5.2 Any performance dates will be estimates only and time will not be of the essence for the performance of the Services.

5.3 Whilst the Supplier may undertake a review of the Client's software licences provided by a Third Party Licensor, and provide commentary on such licences as part of the Services at no additional cost, under no circumstances will the Supplier be deemed to be offering the Client a licence to use software similar to that provided by such Third Party Licensor.

6. THE SUPPORTED SOFTWARE

6.1 The Supplier shall provide the Services in respect of:

6.1.1 the software listed in the Proposal;

6.1.2 any Customizations (subject always to Section 6.2);

6.1.3 any Fix and/or Patch provided by the Supplier to the Client under the Agreement; and

6.1.4 any other software which the Supplier and Client agree in writing from time to time in accordance with Section 15, provided that period in respect of which support is provided for any such additional software shall be consistent with the Term,

(together, the "**Supported Software**").

6.2 If an Incident arises in respect of any Customization implemented by or on behalf of the Client on or after the Support Commencement Date, and such defect occurs within the first three (3) months of such implementation, the Client shall, in the first instance, require the developer of such Customization to remedy the Incident.

7. ACCESS TO SYSTEMS

7.1 The Supplier and the Supplier's Personnel may gain access to the Client's test version of its Systems (**"Test Systems"**), either directly or remotely (“**Access**”) where such Access is granted by the Client, and may only utilize that Access as is required for the proper performance of the Supplier’s obligations under the Agreement. For clarity, the parties acknowledge that the Supplier's Access shall, unless otherwise granted by the Client, be limited to access to and use of the Test Systems and the Supported Software in a test environment.

7.2 Where the Client does not grant Access, the Client acknowledges that the Supplier: (i) may not be able to provide all or part of the Services and/or any required Patches or Fixes; and (ii) shall not be liable for any such failure (including any failure to meet the Service Levels and/or any liability to pay Service Credits).

7.3 Where the Client grants the Supplier Access, the Client hereby grants the Supplier a non-exclusive, sub-licensable, royalty-free license to access and use the Test Systems and the Supported Software in a test environment for the purposes of the Supplier providing the Services and otherwise performing its obligations and exercising its rights under and in connection with this Agreement. The Systems shall remain the property of the Client (or its licensors or lessors).

7.4 The Supplier and the Supplier’s Personnel shall comply with all Client policies agreed in writing by the Supplier from time to time in relation to Access.

7.5 The Supplier shall use commercially reasonable efforts not to introduce any software virus, spyware, Trojan horse, malware or other limiting or disabling code, design or routine that allows unauthorized use of, or access to, or that is otherwise harmful to, any IT system or data (together a **"Virus"**) into the Systems. This obligation may be discharged by maintaining and operating reasonably up to date versions of virus protection and firewall software which are of reasonably acceptable industry standards.

8. CLIENT OBLIGATIONS

8.1 The Client shall:

8.1.1 cooperate with the Supplier in all matters relating to the Services and provide in a timely manner such information relating to the System and Supported Software or access to Client Personnel as the Supplier may require, and shall ensure that any such information is and remains complete and accurate in all respects throughout the Term;

8.1.2 where applicable and subject to Section 7.1, ensure that the Supplier is able to remotely access the Test System and the Supported Software in a test environment (unless agreed otherwise) in order to perform the Services (including maintaining appropriate environmental and operational conditions, and meeting any system requirements specified by the Supplier from time to time);

8.1.3 be solely responsible for ensuring it has all necessary licenses and consents in relation to the System and the Supported Software (including Third Party Licensor licenses) to enable the Supplier to perform the Services in compliance with this Agreement and all relevant Laws and without infringing the Intellectual Property Rights of any third party in relation to the System and/or the Supported Software;

8.1.4 not introduce any Virus into the Supplier's systems;

8.1.5 without affecting its other obligations under the Agreement, comply with all applicable Laws with respect to its activities under the Agreement, including ensuring that all Client Data complies with all applicable Laws;

8.1.6 carry out all its responsibilities set out in the Agreement in a timely and efficient manner; and

8.1.7 to the extent permitted by applicable Laws and except as otherwise expressly provided in this Agreement, be solely responsible for (i) procuring, maintaining and securing its network connections and telecommunications links from its Systems to the Supplier's data centers, and (ii) all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Client's network connections or telecommunications links or caused by the internet.

8.2 The Client shall not use the Services (including by accessing, storing, distributing or transmitting any material through its use of the Services) in a way that is unlawful (including promoting or facilitating unlawful activity), offensive, immoral, harmful, threatening, defamatory, obscene, infringing, harassing, or discriminatory. The Supplier may, without liability to the Client and without prejudice to its other rights or remedies, disable the Client's access to the Services if the Client is in breach of this Section 8.2.

8.3 The Client shall not:

8.3.1 except as may be allowed by any applicable Laws which are incapable of exclusion by agreement between the parties and except to the extent expressly permitted under the Agreement:

(a) attempt to copy, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Services in any form or media or by any means; or

(b) attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Services;

8.3.2 license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit the Services, or otherwise make them available to any third party; or

8.3.3 attempt to obtain, or assist third parties in obtaining, access to the Services.

8.4 The Client shall prevent any unauthorized access to, or use of, the Services. In the event of any such unauthorized access or use, the Client shall notify the Supplier immediately.

9. DEFAULT BY THE CLIENT

9.1 To the extent that the Supplier's performance of any of its obligations under the Agreement is prevented or delayed by a failure or delay by the Client or any of the Support Partners in: (i) complying with this Agreement (including any Client responsibilities set out in the Proposal); and/or (ii) granting the Supplier Access, the Supplier shall be entitled to an extension of time in respect of the performance of the affected obligation commensurate with the delay caused by the Client's or its Support Partner's failure to so comply or delay in complying or failure to grant or delay in granting Access.

10. RELATIONSHIP WITH SUPPORT PARTNERS

10.1 **THE CLIENT SHALL:**

10.1.1 on or immediately after the Support Commencement Date provide the Supplier with details of all Support Partners;

10.1.2 procure that the Supplier is provided with such access to and assistance from all Support Partners as is set out in the Service Level Agreement or otherwise required by the Supplier for the purposes of providing the Services; and

10.1.3 procure that all Support Partners shall cooperate fully with the Supplier as reasonably required for the purposes of providing the Services; and

10.1.4 ensure that its Support Partners do not commit any act or omission which would invalidate the Client's agreement with a Third Party Licensor.

10.2 **THE CLIENT SHALL ENSURE THAT ITS SUPPORT PARTNERS:**

10.2.1 comply with the terms of the Agreement;

10.2.2 fully understand the scope of the Services provided by the Supplier;

10.2.3 raise any issues relating to the Supported Software, including any Incidents, on the Client's behalf with the Supplier in the first instance in accordance with the Service Level Agreement; and

10.2.4 do not raise any such issues or Incidents in relation to the Supported Software with any Third Party Licensor without the Supplier's prior written consent.

10.3 Where the Supplier has consented in writing to its Confidential Information being disclosed to a Support Partner under Section 19.1.2, the Client shall ensure that: (a) the Support Partner is made aware of the confidential nature of the Confidential Information; and (b) the Client and the Support Partner have entered into legally binding confidentiality and non-use obligations equivalent to those set out in Section 19.

10.4 Where any issue or Incident is raised by a Support Partner with the Supplier under Section 10.2, the Supplier shall provide support services (as described in the Proposal) to the Support Partner (including, where appropriate, by providing any Fixes) on the behalf of the Client.

11. RELATIONSHIP WITH THIRD PARTY LICENSORS

11.1 Any Intellectual Property Rights in the Supported Software which are proprietary to a Third Party Licensor shall at all times remain vested in such Third Party Licensor.

11.2 It is the Client's sole responsibility to ensure that it complies with any terms and conditions imposed upon it by any Third Party Licensor in relation to the Supported Software or the support thereof (**"License Terms"**).

11.3 Except as expressly set out in the Agreement or agreed by the parties in writing, the Supplier shall not be obliged itself or on behalf of the Client to download, store or receive from the Client any software, documentation or other work or material which is proprietary to a third party (including: patches, object and source code; documentation and training materials; user interfaces and screen captures of those interfaces; system logs, application logs, traces, or diagnostic reports; design documents; data including metadata, demo data, training data; and/or formatted output and reports). The Supplier shall be relieved of its obligations to perform the Services to the extent that the performance is reliant upon the Supplier downloading, storing or receiving any such materials.

12. CLIENT DATA

12.1 The Client shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of any of the Client's proprietary information or images in the Systems or otherwise provided by the Client to the Supplier in connection with the Services (the **"Client Data"**).

12.2 The Supplier shall not be responsible for the back-up of any Client Data, and the Client hereby acknowledges that it is responsible for maintaining its own database and back-up of any Client Data. In the event of any loss or damage to Client Data, the Client's sole and exclusive remedy against the Supplier shall be for the Supplier to use commercially reasonable efforts to restore the lost or damaged Client Data from the latest back-up of such Client Data maintained by the Supplier in accordance with its standard disaster recovery procedure (for clarity, to the extent such loss or damage was caused wholly and directly by the Supplier). The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Client Data caused by the Client or any third party.

12.3 The Client shall defend, indemnify and hold harmless the Supplier and any company or other entity which directly or indirectly Controls, is Controlled by or is under common Control with the Supplier against any Losses arising out of or in connection with: (a) the Client's (or the Support Partner's) use of the Services in breach of this Agreement;

(b) any claim that the Supplier's (or any of its subcontractor's) use of the Client Data in accordance with the Agreement infringes any applicable Laws or the Supplier's or a third party's Intellectual Property Rights; and (c) any claim that the Supplier's provision of the Services, or the exercise of the Supplier's rights or the performance of its obligations, under or in connection with this Agreement infringes the rights of any third party, including any breach of Section 8.1.3 and/or 17.3.2.

13. INTELLECTUAL PROPERTY RIGHTS

13.1 All Intellectual Property Rights in the Client Data are and will remain, as between the parties, the property of the Client. The Client hereby grants to the Supplier a non-exclusive, sub-licensable, royalty-free license to use the Client Data as necessary to carry out the Supplier's obligations under the Agreement.

13.2 All Intellectual Property Rights in the Services and in any portal or dashboard provided by the Supplier in connection with the Services will belong to the Supplier. The Supplier hereby grants to the Client a non-exclusive, limited, royalty-free license to use such portal and dashboard as necessary during the Term to enjoy the benefit of the Services.

13.3 All Intellectual Property Rights in any Customizations developed by the Supplier and in any Fixes are and will remain, as between the parties, the property of the Client. The Client hereby grants to the Supplier a non-exclusive, perpetual, irrevocable, sub-licensable, worldwide, royalty-free license to use such Customizations and Fixes (including after termination or expiration of the Agreement) as necessary for the Client to enjoy the benefit of the Supported Software and/or Services (as applicable).

13.4 Neither party will have any right or license in respect of the other's Intellectual Property Rights other than as expressly set out in the Agreement. On termination or expiration of the Agreement (or on cancellation or discontinuance of any Services to which those Intellectual Property Rights relate) all rights and licenses granted in respect of such Intellectual Property Rights shall automatically terminate.

14. IPR INFRINGEMENT

14.1 In performing the Services, the Supplier shall not be obliged to take any action which may infringe the Intellectual Property Rights of any Third Party Licensor or any other third party. Subject to Section 14.3, if any Services, Fixes or Patches provided by the Supplier are held or alleged to infringe, or the Supplier believes that they may infringe, a Third Party Licensor's or any other third party's Intellectual Property Rights (an **"Infringing Item"**), the Supplier may, as the Client's sole remedy and at the Supplier's option and expense, either: (a) modify the Infringing Item so that it becomes non-infringing while otherwise substantially complying with the requirements of the Agreement; or (b) replace the relevant Infringing Item with other non-infringing items having a capability materially equivalent to the Infringing Item.

14.2 The Client shall notify the Supplier promptly upon becoming aware of any existing or alleged existence of an Infringing Item.

14.3 In no event shall the Supplier be liable to the Client under Section 14.1 to the extent that any Infringing Item arises as a result of:

14.3.1 a breach of the License Terms or misuse of the Supported Software by the Client;

14.3.2 a modification of the Services, a Fix or a Patch by anyone other than the Supplier;

14.3.3 use of the Services in a manner not specifically permitted by the Agreement or contrary to the instructions given to the Client by the Supplier from time to time; or

14.3.4 use of the Services after notice of the alleged or actual infringement from the Supplier or any appropriate authority or third party.

15. CHANGE CONTROL

15.1 Subject to Section 15.2, if either party requests a change to the Services or the Agreement, the Supplier shall, within a reasonable time, provide a written (including by e-mail) estimate to the Client of:

15.1.1 the likely time required to implement the change;

15.1.2 any variations to the Charges arising from the change; and

15.1.3 any other impact of the change on the terms of the Agreement.

15.2 The Supplier may amend the Services as necessary to comply with any applicable Laws, or if the amendment will not materially affect the nature or quality of the Services.

15.3 If the Supplier requests a change to the scope of the Services, the Client shall not unreasonably withhold or delay consent to it.

15.4 If the Client wishes the Supplier to proceed with the change, the Supplier has no obligation to do so unless the parties have agreed in writing any necessary variations to the Charges and any other relevant terms of the Agreement to take account of the change.

16. CHARGES AND PAYMENT

16.1 In consideration of the provision of the Services, the Client shall pay to the Supplier the charges for the Services, as set out in the Quotation, and any other charges agreed between the parties in respect of services to be provided by the Supplier (together, the **"Charges"**) in accordance with this Section 16.

16.2 16.2 Maximum Compensation. The maximum compensation payable to the Supplier under this Agreement is $1,255,467.68 for the Initial Term of this Agreement. In the event this Agreement is extended for its first optional Subsequent Term ("Year 4"), the total compensation payable to the Supplier under this Agreement is $1,673,450.99. In the event this Agreement is extended for its final Subsequent Term ("Year 5"), the total compensation payable to the Supplier under this Agreement is $2,103,973.80. In the event the total maximum compensation amount in the Initial Term, Year 4, and/or Year 5 is not fully expended, the remaining unspent funding amounts shall roll over to each subsequent term's established maximum compensation.

16.3 The Supplier acknowledges that the County is a local government entity, and does so with notice that the County's powers are limited by the California Constitution and by State law, and with notice that the Supplier may receive compensation under this Agreement only for services performed according to the terms of this Agreement and while this Agreement is in effect, and subject to the maximum amount payable under this section. The Supplier further acknowledges that County employees have no authority to pay the Supplier except as expressly provided in this Agreement

16.4 The Client may increase the software in support by up to 10% during the term of a Proposal without incurring additional charges. Where the Client requests a decrease in the supported software by more than 10% from that set out in the relevant Proposal, the Supplier shall adjust the Charges accordingly for any Subsequent Term, subject to the maximum compensation amount as reflected in Section 16.2.

16.5 The Supplier shall be entitled to invoice the Charges annually in advance on or around the Agreement Date and on each anniversary thereof.

16.6 The Client shall pay each invoice submitted to it by the Supplier in full, in the currency in which the invoice is issued and in cleared funds, within forty five(45) days of the date of the invoice. Time for payment of the Charges by the Client shall be of the essence of the Agreement. Payments shall be made by electronic BACS transfer or such other method as is specified by the Supplier from time to time.

16.7 All amounts payable under the Agreement shall be exclusive of any relevant state or local sales taxes, which shall be paid at the rate and in the manner for the time being prescribed by law and which shall be added by the Supplier to its invoices at the appropriate rate.

16.8 If the Client disputes any Charges, it shall nevertheless pay the relevant invoices in full and the parties shall attempt to resolve the dispute in accordance with Section 0. The Client may not deduct or withhold payment of any sum by reason of any set-off of any claim or dispute with the Supplier whether relating to the quality or performance of the Services or otherwise.

16.9 Without limitation to any other right or remedy available to the Supplier, if the Client has failed to pay any invoice issued under the Agreement in accordance with this Section 16 by the due date for payment, the Supplier may, without liability to the Client, suspend the provision of the Services.

17. WARRANTIES

17.1 Each party warrants to the other party that:

17.1.1 it has full capacity, power and authority to enter into and perform its obligations under the Agreement and has no conflicting obligations to any third party (whether contractual or otherwise); and

17.1.2 the Agreement is executed by a duly authorized representative of the that party.

17.2 The Supplier warrants to the Client that:

17.2.1 the Services will be performed with reasonable skill and care; and

17.2.2 in providing the Services, it will not knowingly cause the Client to breach the License Terms.

17.3 The Client warrants and represents to the Supplier that:

17.3.1 in performing the Client's obligations under the Agreement, it will exercise reasonable skill and care;

17.3.2 to the best of its knowledge, having made reasonable exhaustive enquiries and investigation, it has in place and shall maintain in place during the Term all licenses of the Supported Software from all relevant Third Party Licensors, and any other licenses, consents, other permissions, necessary to enable the Client to receive the benefit of the Services in accordance with the Agreement and has full authority to license or sub-license the Supported Software to the Supplier to the extent necessary for the purposes of providing the Services;

17.3.3 by entering into, and performing its obligations under, the Agreement, including by permitting the Supplier to access and/or use the Supported Software for the purposes of providing the Services, the Client will not be in breach of any License Terms or other applicable agreement; and

17.3.4 the performance of the Services by the Supplier in accordance with the Agreement will not infringe the Intellectual Property Rights of any Third Party Licensor or any other person.

17.4 The Supplier shall not be liable for any failure to comply, or delay in complying, with its obligations under Section 17.2 or the Agreement to the extent such failure or delay is caused by the Client's or a Support Partner's breach of the Agreement (including a failure to comply, or delay in complying, with any Client responsibilities set out in the Proposal) or use of the Services contrary to the Supplier's instructions and/or the terms of the Agreement. If the Services do not comply with Section 17.2, the Supplier will, at its expense, use commercially reasonable efforts to correct any such non-compliance promptly. Such correction or substitution constitutes the Client's sole and exclusive remedy for any breach of its obligations under Section 17.2.

17.5 The Supplier:

17.5.1 does not warrant or represent that the Client's use of the Services will be uninterrupted or error-free;

17.5.2 is not responsible for the Client's use of the Services; and

17.5.3 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Client acknowledges that the Services may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

17.6 Except for those set out in the Agreement, all conditions, warranties or other terms which might have effect between the parties or be implied or incorporated into the Agreement or any collateral contract, whether by statute, common law or otherwise, are hereby excluded, including the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose and the use of reasonable skill and care.

18. LIMITATION OF LIABILITY

18.1 Nothing in the Agreement shall limit or exclude the liability of either party for:

18.1.1 death or personal injury resulting from negligence;

18.1.2 fraud or fraudulent misrepresentation; or

18.1.3 any other liability which cannot be limited or excluded by law.

18.2 Subject to Section 18.1, the Supplier shall not in any circumstances have any liability to the Client, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, for:

18.2.1 loss of profits;

18.2.2 loss of anticipated savings;

18.2.3 loss of business opportunity;

18.2.4 loss of or damage to goodwill or reputation;

18.2.5 loss of or damage to (including corruption of) data; or

18.2.6 indirect, consequential or special loss or damages.

18.3 Subject to Sections 18.1 and 18.2, except as set out in Section 18.1, the Supplier's total liability to the Client, whether in contract (including by way of indemnity), tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with the Agreement shall be limited to and will in no circumstances whatsoever exceed a sum of 100% of the total Charges paid by the Client to the Supplier under the Agreement in the Contract Year in which the liability arose. For the purposes of this Section, a **"Contract Year"** means the consecutive period of twelve (12) months commencing on the Support Commencement Date and each anniversary thereof.

18.4 The Client acknowledges that the limitations and exclusions set out in this Section 18 reflect the level of the Charges and the allocation of risk between the parties.

18.5 The Supplier shall maintain in force, during the term of the Agreement the following insurance policies:

18.5.1 employer's liability insurance for a minimum amount of cover of £10 million on a single event or series of related events in a single calendar year;

18.5.2 professional indemnity insurance for a minimum amount of cover of £5 million on a single event or series of related events in a single calendar year; and

18.5.3 public liability insurance for a minimum amount of cover of £10 million on a single event or series of related events in a single calendar year.

19. CONFIDENTIAL INFORMATION

19.1 Subject to Sections 19.2 to 19.4, a receiving party agrees during the Term and thereafter:

19.1.1 to keep the Confidential Information of the other party in strict confidence and to take all reasonable precautions to prevent the unauthorized disclosure of it to any third party;

19.1.2 not to disclose any of the other party's Confidential Information in whole or in part to any third party except with the prior written consent of the disclosing party or as otherwise expressly permitted by any other Section of the Agreement; and

19.1.3 not to use any of the Confidential Information for any purpose other than as necessary to fulfil its obligations under the Agreement without the prior written consent of the disclosing party.

19.2 The receiving party may disclose the Confidential Information to such of its Personnel or legal or professional advisors who reasonably require access to it for the purpose of fulfilling the receiving party's obligations under the Agreement provided that before any of the Confidential Information is disclosed to them, they are made aware of its confidential nature and that they are under a legally-binding obligation to the receiving party to treat that Confidential Information in the strictest confidence which is equivalent to the terms of the Agreement. The receiving party will be liable to the disclosing party for any disclosure or misuse of the Confidential Information by the receiving party's Personnel or advisors.

19.3 The obligations of confidence and non-use set out in Section 19.1 will not apply to any Confidential Information which was at the time of disclosure or other becomes:

19.3.1 published, known publicly or otherwise in the public domain or known to and at the free disposal of the receiving party in circumstances in which the receiving party has no reason to believe that there has been a breach of an obligation of confidence owed to the disclosing party; or

19.3.2 is independently developed by or on behalf of the receiving party without use of or reliance on the Confidential Information received from the disclosing party.

19.4 Neither party will be in breach of its obligations under Section 19.1 to the extent that it is required to disclose any Confidential Information of the other under any Law or by or to a court or other public, regulatory or financial authority that has jurisdiction over it, provided that unless prohibited by any Law from doing so the receiving party gives the disclosing party written notice prior to disclosing any of the Confidential Information and that the disclosure is made only to the extent required and for the purpose of complying with the requirement and that the receiving party takes all reasonable measures to ensure, as far as it is possible to do so, the continued confidentiality of any Confidential Information so disclosed.

20. PUBLICITY

20.1 The Supplier may refer to the Client as being a client of the Supplier, including on its website and in customer reference lists and sales presentations. The Client hereby grants the Supplier a perpetual, irrevocable license to use the Client's logo for such purpose.

20.2 The Client hereby agrees to act as a reference for the Supplier and the Supplier shall be entitled to write and publish a case study about its provision of the Services to the Client.

21. DATA PROTECTION

21.1 For the purposes of this Section, **"Privacy and Data Protection Laws"** means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of personal data including: (i) any U.S. federal or state laws, such as the Gramm-Leach-Bliley Act, the Health Insurance Portability & Accountability Act and the California Consumer Privacy Act (CCPA); (ii) EU Regulation 2016/679 (**"EU GDPR"**); (iii) GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the **"UK GDPR"**); (iv) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the EU GDPR; (v) in the UK, the Data Protection Act 2018 (**"DPA"**); (vi) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC); and (vii) in the UK, the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time; and the terms "data subject", "personal data", "processing", "processor" and "controller" shall have the meanings set out in the DPA;

21.2 Data Security. The Supplier shall be responsible for the privacy and security safeguards, as identified in Exhibit C, entitled "Data Security." To the extent required to carry out the assessment and authorization process and continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any County data collected and stored by the Supplier, the Supplier shall afford the County access as necessary at the Supplier's reasonable discretion, to the Supplier's facilities, installations, and technical capabilities. If new or unanticipated threats or hazards are discovered by either the County or the Supplier, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

21.3 .Each party shall comply with the provisions and obligations imposed on it by the Privacy and Data Protection Laws when processing personal data in connection with this Agreement. Such processing shall be in respect of the following:

21.3.1 **Nature and purpose of processing**: incidental access to personal data in the performance of the Services;

21.3.2 **Categories of personal data and data subjects**: such personal data as is held in any IT environment to which the Supplier to which the Supplier is granted access in order to perform the Services, and the individuals to which such personal data relates;

21.3.3 **Duration**: only so long as necessary for the purposes of providing the Services.

21.4 To the extent that a party processes any personal data on behalf of the other party, the processing party shall: (a) comply with the provisions and obligations imposed on a processor by the UK GDPR and/or EU GDPR (as applicable), including the stipulations set out in Article 28(3)(a)-(h) which form a part of, and are incorporated into, this Agreement as if they were set out in full, and the reference to "documented instructions" in Article 28(3)(a) shall include the provisions of this Agreement; and (b) not disclose any personal data to any data subject or to a third party other than at the written request of the other party or as expressly provided for in this Agreement.

21.5 If either party receives any complaint, notice or communication which relates to the processing of personal data by the other party or to either party's compliance with the Privacy and Data Protection Laws, or if any Personal Data processed in connection with this Agreement is subject to a personal data breach (as defined in the UK GDPR), the relevant party shall immediately notify the other party and provide the other party with reasonable co-operation and assistance in relation to any such complaint, notice, communication or personal data breach.

22. EXPORT

22.1 Neither party shall export, directly or indirectly, any technical data acquired from the other party under the Agreement (or any products, including software, incorporating any such data) in breach of any applicable export control Laws ("**Export Control Laws**").

22.2 Each party undertakes:

22.2.1 contractually to oblige any third party to whom it discloses or transfers any such data or products to make an undertaking to it in similar terms to the one set out above; and

22.2.2 if requested, to provide the other party with any reasonable assistance, at the reasonable cost of the other party, to enable it to perform any activity required by any competent government or agency in any relevant jurisdiction for the purpose of compliance with any Export Control Laws.

23. TERMINATION

23.1 Either party may at any time terminate the Agreement and/or cancel or discontinue any Services (in whole or in part) with immediate effect by giving written notice to the other party if:

23.1.1 the other party fails to pay any amount due under the Agreement on the due date for payment and such amount remains unpaid for not less than fourteen (14) days after the due date for such payment;

23.1.2 the other party commits a material breach of any term of the Agreement and (if such breach is remediable) fails to remedy that breach within a period of thirty (30) days after being notified in writing (including by e-mail) to do so;

23.1.3 the other party or any of its holding companies becomes insolvent or has a receiver, administrative receiver, administrator or similar officer appointed or applies for or has called a meeting of creditors or resolves to go into liquidation (except for a bona fide amalgamation or reconstruction while solvent where the resulting entity agrees to be bound by and assumes that party's obligations under the Agreement) or has a petition lodged against it in relation to any potential insolvency which is not successfully opposed within thirty (30) days of being lodged or an application is made to appoint a provisional liquidator of the other party or an administration order or notice of intention to appoint an administrator is given in relation to the other party or a proposal is made for a voluntary arrangement or any other composition, scheme or arrangement with or assignment for the benefit of any of the other party's creditors or any event analogous to any of the foregoing occurs in any jurisdiction; or

23.1.4 the other party ceases or threatens to cease to carry on its business.

23.2 The Supplier may, without prejudice to its other rights or remedies, terminate the Agreement immediately by notice to the Client if the Client:

23.2.1 undergoes a change of Control;

23.2.2 sells all of its assets or is merged or re-organised in circumstances where it is not the surviving entity; or

23.2.3 disputes the ownership or validity of the Supplier's Intellectual Property Rights.

23.3 The Client may, without prejudice to its other rights or remedies, terminate the Agreement for non-allocation of funds. The terms of this Agreement are contingent on the approval of funds by the appropriating government agency. If sufficient funds are not allocated, then the Client, upon thirty days advance written notice to the Supplier may:

23.3.1 Modify the services provided by the Supplier under this agreement; or

23.3.2 Terminate this Agreement.

23.4 Subject to clause 23.1, the Client may terminate the Agreement by giving the Supplier at least six months' written notice, provided that the client shall, within thirty days of termination of the Agreement under this Section 23.4, pay to the Supplier all unpaid Charges that would otherwise have been due to the Supplier in the Initial Term and each Subsequent Term (as applicable) but for such termination.

24. CONSEQUENCES OF TERMINATION

24.1 Termination or expiration of the Agreement shall not limit any of the parties' rights, remedies, liabilities and obligations which have accrued as at termination or expiration. Other than as set out in the Agreement, neither party shall have any further obligation to the other under the Agreement after its termination.

24.2 On termination or expiration of the Agreement for any reason:

24.2.1 the Client shall immediately cease use of the Services;

24.2.2 save to the extent a party is required to retain a copy under applicable Laws or pursuant to its bona fide internal record-keeping policies, each party shall delete or return (at the other party's option) the other party's Confidential Information;

24.2.3 the Client shall immediately pay any outstanding unpaid invoices and interest due to the Supplier; and

24.2.4 the Client shall not be entitled to any refund of Charges.

24.3 If requested by the Client, and save where the Supplier has terminated this Agreement for cause, the Supplier will (at the Supplier's then current rates) provide the Client with such reasonable assistance as is specified in the any exit plan that may be agreed in writing between the parties in relation to the migration of the Services to the Client or to any replacement supplier for such period as the parties may agree in writing.

24.4 Notwithstanding the expiration or termination of the Agreement for any reason, it shall continue in force to the extent necessary to give effect to those of its provisions which expressly or by implication have effect after expiration or termination, including Sections 1, 13.3 18, 19, 23.4, 24, 26, 0, 28, 29, 30, 32, 33.

25. NON-SOLICITATION

25.1 Neither party shall, without the prior written consent of the other party, at any time from the date of the Agreement to the expiration of six (6) months after the end of the Term, solicit or entice away from the other party or employ or attempt to employ any person who is, or has been, employed by the other party during the Term. This Section 25.1 will not apply to and shall not prevent any party from hiring any person by means of an advertising campaign which is not specifically targeted at any of the staff of the other party.

26. NOTICES

26.1 Any notice to be given under the Agreement must be in writing (including e-mail) and may be delivered to the other party by any of the methods set out in the left hand column below to (in the case of the Supplier) Support Revolution Inc., 111 Congress, Suite 500, Austin, Texas (addressed FAO Chief Commercial Officer and a copy sent to info@supportrevolution.com) and (in the case of the Client) to the Client's registered office address (or such other address or email address as is notified by either party from time to time in accordance with this Section), and will be deemed to be received on the corresponding day set out in the right hand column:

Method of service	**Deemed day of receipt**
By hand or courier	the day of delivery
By pre-paid first class post or recorded delivery	the second working day after posting in the country of receipt
By email	one hour after completion of transmission by the sender (save where the email receives an automated response that it is undelivered or undeliverable in which event this deeming provision shall not apply)

26.2 The person and their address having authority to give and receive notices provided for or permitted under this Agreement for the County include: the Director of Internal Services/Chief Information Officer at 333 W. Pontiac Way, Clovis, CA and a copy sent to isdcontracts@fresnocountyca.gov.

27. DISPUTE RESOLUTION

27.1 It is the intention of the parties to settle amicably by negotiation all disagreements and differences of opinion on matters of performance, procedure and management arising out of the Agreement ("**Disputes**").

27.2 In relation to any Dispute a party may follow the dispute resolution procedure set out in this Section:

27.2.1 either party may give to the other written (including e-mail) notice of the Dispute, setting out its nature and full particulars ("**Dispute Notice**)", together with relevant supporting documentation. On service of the Dispute Notice the Account Manager and the Client Representative shall attempt in good faith to resolve the Dispute; and

27.2.2 if the Account Manager and the Client Representative are for any reason unable to resolve the Dispute within fourteen (14) days of service of the Dispute Notice, the Dispute may be referred to a director of the Supplier and a director of the Client, who shall attempt in good faith to resolve it.

28. ASSIGNMENT AND SUBCONTRACTING

28.1 The Client shall not assign, novate, transfer, charge, sublicense, subcontract or otherwise deal in or dispose of any of its rights and obligations under the Agreement, in whole or in part, without the Supplier's prior written consent.

29. THIRD PARTY RIGHTS

29.1 The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under the Agreement is not subject to the consent of any person that is not a party to the Agreement.

30. FORCE MAJEURE

30.1 The Supplier shall not in any circumstances be in breach of the Agreement nor liable for any delay in performing, or failure to perform, any of its obligations under the Agreement if such delay or failure results from any event beyond its reasonable control (each a **"Force Majeure Event"**) and, and in such circumstances the Supplier shall be entitled to a reasonable extension of the time for performing such obligations.

30.2 If the Force Majeure Event prevents the Supplier from providing any of the Services for more than twelve (12) weeks, then either party may, without limiting its other rights or remedies, have the right to terminate the Agreement immediately by giving written notice to the other party.

31. ANTI-CORRUPTION AND ANTI-BRIBERY

31.1 The Supplier shall:

31.1.1 comply, and shall ensure that its Personnel comply, with all applicable Laws relating to anti-bribery and corruption, including the U.S. Foreign Corrupt Practices Act(**"Relevant Requirements"**);

31.1.2 have and maintain in place throughout the term of the Agreement its own policies and procedures to ensure compliance with the Relevant Requirements;

31.1.3 promptly report to the Client any request or demand for any undue financial or other advantage of any kind received by the Supplier in connection with the performance of the Agreement; and

31.1.4 notify the Client in writing (including by e-mail) if a foreign public official (as defined in the U.S. Foreign Corrupt Practices Act) becomes an officer or employee of the Supplier or acquires a direct or indirect interest in the Supplier.

31.2 If any member of the Supplier's board of directors is party to a self-dealing transaction, he or she shall disclose the transaction by completing and signing a "Self-Dealing Transaction Disclosure Form" (Exhibit D to this Agreement) and submitting it to the County before commencing the transaction or immediately after.

32. GENERAL

32.1 The rights and remedies provided by the Agreement are cumulative and are additional to any right, power or remedy provided under general law or otherwise.

32.2 If any provision of the Agreement (or part of a provision) is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force.

32.3 If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.

32.4 Each party shall (at its own expense) promptly execute and deliver all such documents, and do all such things, or procure the execution and delivery of all documents and doing of all such things as are required to give full effect to the Agreement and the transactions contemplated by it.

32.5 No variation of the Agreement shall be effective unless it is in writing and signed by the parties (or their authorized representatives).

32.6 Any waiver of any right under the Agreement is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

32.7 No failure to exercise or delay in exercising any right or remedy provided under the Agreement or by law constitutes a waiver of such right or remedy, nor shall it prevent or restrict any future exercise or enforcement of such right or remedy.

32.8 No single or partial exercise of any right or remedy under the Agreement shall prevent or restrict the further exercise of that or any other right or remedy.

32.9 Nothing in the Agreement will be construed as constituting or evidencing any partnership, contract of employment or joint venture of any kind between either of the parties or as authorizing either party to act as agent for the other. Neither party will have authority to make representations for, act in the name or on behalf of or otherwise bind the other party in any way.

32.10 Except as expressly provided, no terms and conditions, standard or otherwise, contained on any invoice, purchase order, order form, license or other document of the Client shall apply to the subject matter of the Agreement unless incorporated as a variation agreed in writing between the parties and signed by the relevant representatives of each party.

32.11 The Agreement and the documents referred to in it constitute the whole Agreement and understanding of the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter of the Agreement. The Client acknowledges that:

32.11.1 in entering into the Agreement it did not rely (and has not relied) on any representation (whether negligent or innocent), statement or warranty (in each case whether written or oral) of any kind made or agreed to by any person (whether a party to the Agreement or not) other that those expressly set out in the Agreement; and

32.11.2 the only remedy available in respect of any misrepresentation or untrue statement made to it shall be a claim for breach of contract under the Agreement.

32.12 The Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of the Agreement, but all the counterparts shall together constitute the same agreement.

32.13 Each party shall bear its own costs and expenses (including legal fees) associated with the preparation of the Agreement.

32.14 The parties agree that this Agreement may be executed by electronic signature as provided in this section.

32.14. 1 An "electronic signature" means any symbol or process intended by an individual signing this Agreement to represent their signature, including but not limited to (1) a digital signature; (2) a faxed version of an original handwritten signature; or (3) an electronically scanned and transmitted (for example by PDF document) version of an original handwritten signature.

32.14.2 Each electronic signature affixed or attached to this Agreement (1) is deemed equivalent to a valid original handwritten signature of the person signing this Agreement for all purposes, including but not limited to evidentiary proof in any administrative or judicial proceeding, and (2) has the same force and effect as the valid original handwritten signature of that person.

32.14.3 The provisions of this section satisfy the requirements of Civil Code section 1633.5, subdivision (b), in the Uniform Electronic Transaction Act (Civil Code, Division 3, Part 2, Title 2.5, beginning with section 1633.1).

32.14.4 Each party using a digital signature represents that it has undertaken and satisfied the requirements of Government Code section 16.5, subdivision (a), paragraphs (1) through (5), and agrees that each other party may rely upon that representation.

32.14.5 This Agreement is not conditioned upon the parties conducting the transactions under it by electronic means and either party may sign this Agreement with an original handwritten signature.

33. GOVERNING LAW AND JURISDICTION

33.1 The Agreement and any dispute or claim arising out of or in connection with it or its subject matter, performance or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of the State of California without reference to conflict of laws provisions thereof. The parties irrevocably agree that the state and federal courts in Fresno, California shall have exclusive jurisdiction to settle any such dispute or claim. As of the date of the Agreement's approval by the Client's governing Board, Supplier shall be registered with the California Secretary of State and in good standing.

This Agreement has been signed by a duly authorized representative of each party on the date appearing below.

Signed for and on behalf of	**Signed for and on behalf of** **Support Revolution Limited**
Signature:	Signature: DocuSigned by: Victoria Molloy AD643474AFF7475...
Name: Nathan Magsig	Name: Victoria Molloy
Title: Chairman of the Boarrd of Supervisors of the County of Fresno	Title: Chief Commercial Officer
Date: 12/17/2024	Date: 18-Nov-24 | 12:50 AM PST

Attest:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: Kelly Hancock
Deputy

For accounting use only:

Org No.: 8933
Account No.: 7309
Fund No.: 1030
Subclass No.: 10000

Exhibit A

1. Executive Summary

This document details the Support Revolution PeopleSoft third-party support and maintenance service.

1.1 How Our Support Works

The Support Revolution service has been designed to replace the PeopleSoft support and maintenance service from other vendors and improve it to deliver a better customer experience.

We provide the Support Revolution service to customers for as many years as they wish, with no forced upgrades and no de-support dates, so there will be no need to go through any more complex, costly and time-consuming upgrades. We also support customisations made to our customers' systems at no additional charge, provided that they have gone through a robust development and testing process.

This document outlines the third-party support service.

2. Raising A Service Request

2.1 Step One: You contact our Service Desk with an issue

The first step to getting support is telling us that there is a problem.

Our Service Desk system is based on Remedyforce, one of the leading Service Desk applications in the world. Remedyforce is Cloud-based, and we have configured it specifically to support our customers' needs, making sure it is intuitive to use and that it provides all the options you would expect from a world-class support system.

You and your team can contact the Service Desk 24/7 through the following methods:

- **Self-service ticketing in Remedyforce**: Your team can login to Remedyforce to review any open tickets or create new ones. The process to do this is very intuitive, but we also provide a series of videos and guides to assist your team.
- **Email**: Your team can email a dedicated address to open or respond to tickets in Remedyforce. Any new tickets are automatically forwarded and assigned to the right people, so you never have to keep re-explaining the issue.
- **Telephone**: We have a dedicated phone line to our global support team who are on hand to answer questions, provide live support, or create/respond to your tickets.

When a call/email/ticket is raised to the Service Desk, the Service Desk Manager 'triages' the incident and depending on the resource required, will then allocate it to a consultant with the appropriate level of skill, expertise and availability. An automated email is then generated and sent to the person that raised the incident to inform them of the details of the Service Desk ticket including the unique ticket number, date, time raised and the description of the issue.

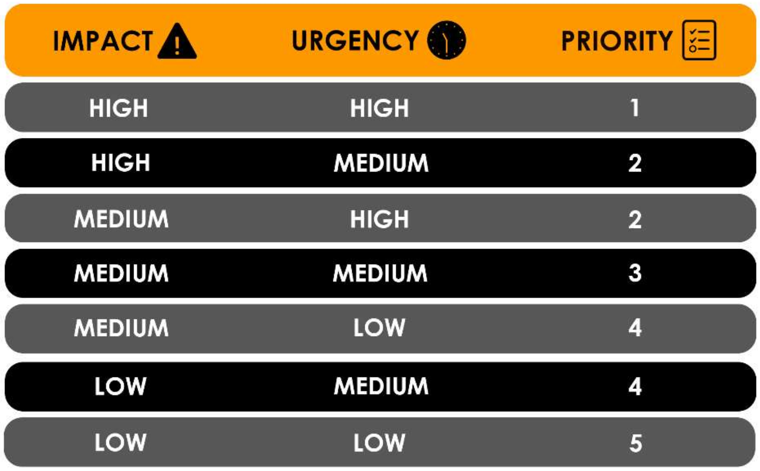
We also provide our own knowledge base of self-service guides and tutorials that your team can use to diagnose and solve issues themselves if they prefer.

2.2 Step Two: Your issue is assigned a response and resolution target

Our Remedyforce service desk system and the processes surrounding it are based on ITIL best practice. During the 'triage' process that the Service Desk Manager carries out for each incident, it is allocated an *Impact* (High, Medium or Low) and an *Urgency* (High, Medium or Low). These definitions are agreed with you and re-confirmed for each new ticket.

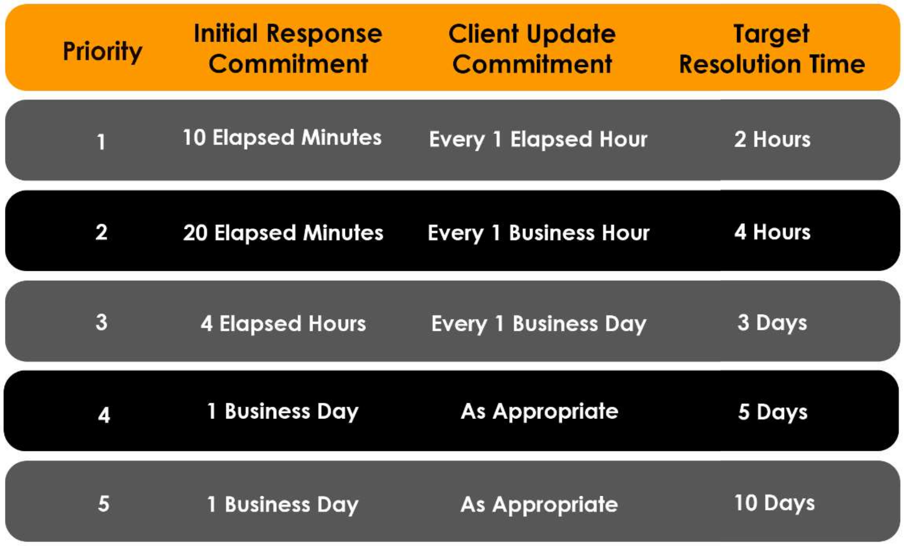
Exhibit A

The combination of *Impact* and *Urgency* defines the *Priority* of an incident as follows:



IMPACT	URGENCY	PRIORITY
HIGH	HIGH	1
HIGH	MEDIUM	2
MEDIUM	HIGH	2
MEDIUM	MEDIUM	3
MEDIUM	LOW	4
LOW	MEDIUM	4
LOW	LOW	5

The agreed Priority of the ticket impacts our service level targets, which are defined in a Service Level Agreement (SLA). These SLAs are embedded within our Remedyforce Service Desk system and are used by the system to monitor our performance.
Our standard SLA includes the following Initial Response and Target Resolution Times:



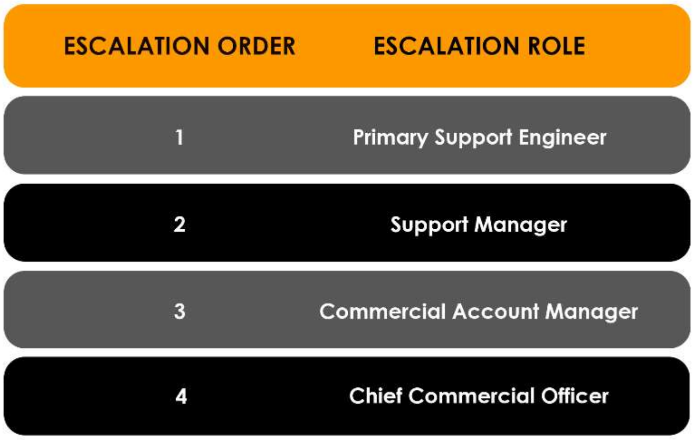
Priority	Initial Response Commitment	Client Update Commitment	Target Resolution Time
1	10 Elapsed Minutes	Every 1 Elapsed Hour	2 Hours
2	20 Elapsed Minutes	Every 1 Business Hour	4 Hours
3	4 Elapsed Hours	Every 1 Business Day	3 Days
4	1 Business Day	As Appropriate	5 Days
5	1 Business Day	As Appropriate	10 Days

Critical incidents are subject to the highest level of commitment in our Service Level Agreement, with an Initial Response Commitment of 10 elapsed minutes, a Client Update Commitment of every 1 elapsed hour, and a Target Resolution Time of 2 hours.
To ensure we meet our SLAs, incidents are automatically escalated within the support team as they approach their resolution targets. In addition, incidents may be escalated by a client when we have been unable to resolve an issue within the target resolution time, or when the client needs to raise the priority of that issue. An incident is escalated via the Service Desk Manager.
Whilst we guarantee to respond in 10 minutes, your team can call our support team on a dedicated number and be put straight through to one of our Service Desk Managers. They will then triage the incident with you before allocating the incident to an engineer with the appropriate levels of skills and expertise to assist you. The engineer will engage with you immediately and work to resolve the issue. We offer a bespoke support service where our

engineers will seek to identify the root cause of each issue so that we address the underlying problem rather than simply addressing the symptoms. Should the incident still be ongoing at the end of the engineer’s shift, they will have a full briefing session with the engineer on the next shift. We operate three 9-hour shifts in each 24-hour period to allow 30-minute handover calls between shifts.

For critical incidents, we have a separate Major Incident Process which is detailed in the Support Revolution Operating Manual. Major Incidents have a Major Incident Manager that coordinates communications and updates for both organisations and remains in place until the issue is resolved. On resolution, they are responsible for the creation and distribution of a Major Incident Report containing a full Root Cause Analysis (RCA).

Your team can escalate any incident at any time. The first point of escalation is to your dedicated Primary Support Engineer who selects the team that provides support to you and manages them. Should you wish to escalate the issue further, it then goes to your Support Manager, then your Commercial Account Manager and finally to the Chief Commercial Office, who sits on our Board of Directors.



ESCALATION ORDER	ESCALATION ROLE
1	Primary Support Engineer
2	Support Manager
3	Commercial Account Manager
4	Chief Commercial Officer

2.3 Step Three: Our 24/7 team begins to tackle the issue

Once an incident has been raised and added to our Service Desk, our team begins working on it. Each incident is given a priority and assigned to one of our consultants who will then work towards resolving the incident within the agreed SLA timeframes.

We use a "follow-the-sun" methodology, meaning you can always contact a qualified member of the team who will be aware of and actively working on your incident. You will still have a single dedicated consultant who will own the ticket, but they will seamlessly handover the details as shifts change to ensure that there are no service interruptions or delays.

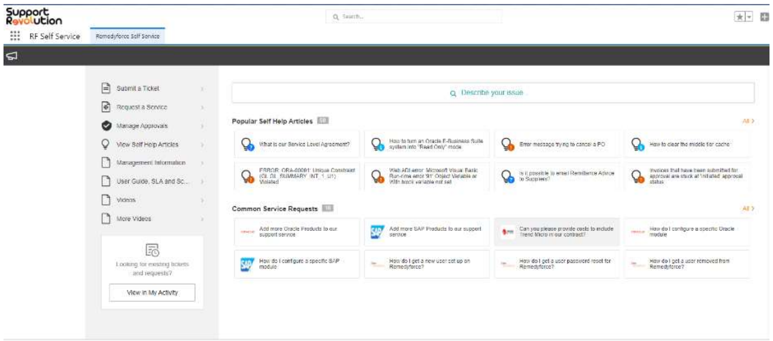
We only employ experienced professionals; all Support Revolution consultants have a minimum of 15 years' experience. We do not employ apprentices to work on the Service Desk as we believe that a quality service can only be provided by experienced professionals.

2.4 Step Four: You are kept informed of progress

Throughout the lifetime of an incident, we provide regular progress updates. Each time an incident is updated on our system, an automated email is sent out to indicate that an update has been made. Regular updates are also provided by telephone by our Service Desk staff. The frequency of updates varies with the severity of the incident and are detailed in the Client Update Commitments within our SLA.

(a) Remedyforce Reporting

Our Remedyforce system includes a Customer Portal so you can track the progress on any incident.



Popular Self Help Articles

- What is our Service Level Agreement?
- How to turn an Oracle E-Business Suite system into "Read Only" mode
- Error message trying to cancel a PO
- How to clear the middle tier cache
- ERROR: ORA-00001: Unique Constraint (GL.GL_SUMMARY_INT_1_U1) Violated
- Web ADI error: Microsoft Visual Basic Run-time error '91' Object Variable or With block variable not set
- Is it possible to email Remittance Advice to Suppliers?
- Invoices that have been submitted for approval are stuck at 'Initiated' approval status

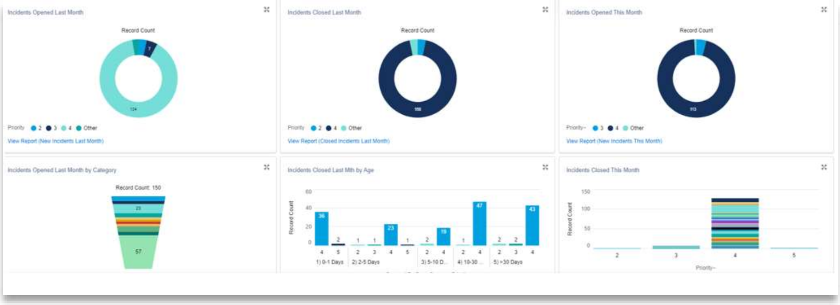
Common Service Requests

- Add more Oracle Products to our support service
- Add more SAP Products to our support service
- Can you please provide costs to include Trend Micro in our contract?
- How do I configure a specific Oracle module
- How do I configure a specific SAP module
- How do I get a new user set up on Remedyforce?
- How do I get a user password reset for Remedyforce?
- How do I get a user removed from Remedyforce?

Exhibit A

This portal allows users to submit and track tickets, access our self-service reporting, and access our self-help guides and tutorials.

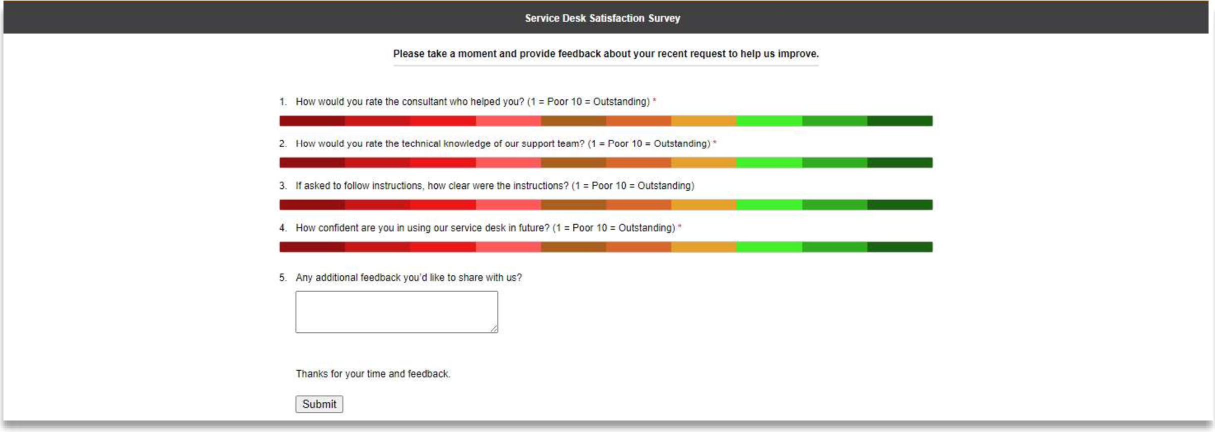
The Remedyforce system includes detailed reporting of tickets raised and closed, our SLA performance, and much more. Data is gathered automatically and displayed in dashboards like the one below:


Incidents Opened Last Month
Record Count
7
124
Priority ● 2 ● 3 ● 4 ● Other
View Report (New Incidents Last Month)
Incidents Closed Last Month
Record Count
168
Priority ● 2 ● 4 ● Other
View Report (Closed Incidents Last Month)
Incidents Opened This Month
Record Count
113
Priority ● 3 ● 4 ● Other
View Report (New Incidents This Month)
Incidents Opened Last Month by Category
Record Count: 150
23
57
Incidents Closed Last Mth by Age
Record Count
60
40
20
0
36
2
1
1
23
1
2
19
1
47
2
2
43
4 5 2 3 4 5 2 4 2 4 2 3 4
1) 0-1 Days
2) 2-5 Days
3) 5-10 D...
4) 10-30 ...
5) >30 Days
Incidents Closed This Month
Record Count
150
100
50
0
2 3 4 5
Priority

Customers can click on any of the graphs above to see the underlying reports, which include details of whether we met or missed the SLA on each incident. You can even click on the incident numbers of individual tickets to see the incident report and all calls and emails sent and received on that issue with dates and times, giving a full audit trail.

2.5 Step Five: The issue is resolved

Once an incident is resolved, we request approval from you before we close the ticket. Once closed, the ticket owner (on your side) will be sent an automatic feedback survey to ensure we keep improving our service.



Service Desk Satisfaction Survey

Please take a moment and provide feedback about your recent request to help us improve.

1. How would you rate the consultant who helped you? (1 = Poor 10 = Outstanding) *
2. How would you rate the technical knowledge of our support team? (1 = Poor 10 = Outstanding) *
3. If asked to follow instructions, how clear were the instructions? (1 = Poor 10 = Outstanding)
4. How confident are you in using our service desk in future? (1 = Poor 10 = Outstanding) *
5. Any additional feedback you'd like to share with us?

Thanks for your time and feedback.

Upon closure of any issue, a detailed explanation of the incident may be requested. We will then provide a detailed report from our Service Desk system with details of the problem and the steps employed to resolve it.

2.6 How We Provide Patches and Fixes

(a) General patches and fixes

Where we or our customers uncover bugs and other issues, we may update the PeopleSoft software to provide a fix. As part of the purchase of their licences, customers have had to purchase licences to enable them to customise their system(s) to meet their needs. This entitles our customers and any partner that they choose (such as us), to amend this code as required. We use this mechanism to address any bugs that arise.

We will apply patches directly on your PeopleSoft test system and provide details of the content of the patch. We then support the testing of these patches until they pass user acceptance testing and are promoted to the production system.

We also provide an online Knowledge Base where we publish details of new bug fixes as they are made available, and our Account Managers make our customers aware of these new fixes if they are relevant to them.

(b) Tax, Legal and Regulatory Updates

We are registered with governments, legal and tax authorities across the globe and receive regular updates on any changes way in advance of them coming into force. This includes details on upcoming changes to Payroll legislation in all countries, including all Federal and State changes for customers in North America.

We record these changes on the "Support Revolution Tax Legal and Regulatory Change Manager". This shows all upcoming changes by country, what they do with their effective date. We review these changes at the start of our service and quarterly thereafter with you. We then create a bespoke project plan of the changes that you need and when they are to be delivered.

We create bespoke updates on one of your Test systems, test them and then support your team through user acceptance testing. This ensures that our updates work with your specific configuration and customisations. We deliver the finalised updates with full installation instructions and supporting documentation.

(c) Customisations

We provide support for customisations as part of our standard support offering. Any new customisations are supported after they have been error free for three months from going live. If errors occur within this three-month period, we will ask you to refer the issue back to the team that developed the change. Any changes that are delivered by our team are fully supported from go live.

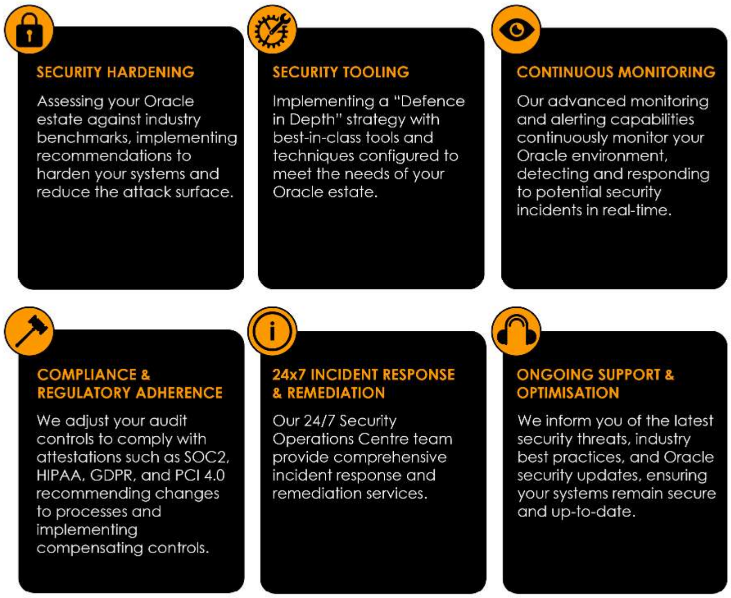
(d) Quality of Service

We are ISO27001 (Information Security) and ISO9001 (Quality) accredited, and our services are delivered to these high international standards. We strive to continuously improve our business processes and the quality of the services that we deliver.

The governance of our processes to support these policies is managed by our Support Manager. The quality and security policy and processes are audited annually by our external auditors.

2.7 Security Patching

Our PeopleSoft Security Hardening, Monitoring, and Protection Service is designed to provide a robust and proactive solution to safeguard your PeopleSoft environment(s). This service combines expert-led assessments, strategic recommendations, and ongoing monitoring to help you mitigate risks, enhance compliance, and maintain the integrity of your Oracle PeopleSoft systems. It comprises:



SECURITY HARDENING

Assessing your Oracle estate against industry benchmarks, implementing recommendations to harden your systems and reduce the attack surface.

SECURITY TOOLING

Implementing a "Defence in Depth" strategy with best-in-class tools and techniques configured to meet the needs of your Oracle estate.

CONTINUOUS MONITORING

Our advanced monitoring and alerting capabilities continuously monitor your Oracle environment, detecting and responding to potential security incidents in real-time.

COMPLIANCE & REGULATORY ADHERENCE

We adjust your audit controls to comply with attestations such as SOC2, HIPAA, GDPR, and PCI 4.0 recommending changes to processes and implementing compensating controls.

24x7 INCIDENT RESPONSE & REMEDIATION

Our 24/7 Security Operations Centre team provide comprehensive incident response and remediation services.

ONGOING SUPPORT & OPTIMISATION

We inform you of the latest security threats, industry best practices, and Oracle security updates, ensuring your systems remain secure and up-to-date.

Security Hardening: Our team of Oracle PeopleSoft security experts will conduct a thorough assessment of your Oracle landscape based on DISA-STIG and CIS Benchmark standards, identifying vulnerabilities and misconfigurations. We will then provide tailored recommendations and implementation support to harden your PeopleSoft systems, reducing the attack surface and strengthening your overall security posture. We then deliver tailored hardening techniques and compensating controls to ensure that your systems can pass penetration testing and auditing.

Security Tooling: We use a "Defence in Depth" strategy to address security vulnerabilities inherent not only with hardware and software but also with people, as negligence or human error are often the cause of a security breach.

For customers that want them, we provide licenses for Trend Micro Deep Security and support the implementation of this toolset across your PeopleSoft estate for an additional cost. This is a virtual patching solution that places a virtual fence around your PeopleSoft systems. Trend issues new rules to address new vulnerabilities weekly on a Tuesday. Customers then apply these rules via the Trend Micro Deep Security console on their estates without the need for regression testing or system downtime. Trend issues urgent rules to fix "Zero Day" vulnerabilities outside of their weekly cycle and as soon as they are available. This approach means that your PeopleSoft estate will be protected much more quickly and to a much higher level than it ever was with Oracle's quarterly Critical Patch Updates (CPUs). For customers that require additional protection, we recommend additional tools including:

- **Waratek Java Security Platform,** to protect both modern and legacy applications & APIs with the only platform that not only stops exploits but also corrects the vulnerable code, eliminating exploitability.

- **Trellix Database Security** which finds and protects sensitive information in databases from accidental leakage and intentional exposure while maintaining security, optimising performance, and managing access.

Continuous Monitoring: For customers that purchase our Trend implementation and monitoring service, our advanced monitoring and alerting capabilities continuously monitor their PeopleSoft environments, detecting and responding to potential security incidents in real-time. This proactive approach helps customers to stay ahead of emerging threats and ensures the timely detection and resolution of security breaches. Our systems issue regular Security Vulnerability Analysis Reports (SVAR's) including Intrusion Prevention Reports and Recommendations Reports. These show any attempted attacks on a customers' systems and recommendations to prevent them.

Compliance and Regulatory Adherence: We will work closely with your teams to ensure your PeopleSoft systems comply with industry standards and regulatory requirements, such as CCPA, GDPR, HIPAA, or SOX. We provide additional consultancy services to adjust your audit controls to comply with attestations such as SOC2, NIST, SSAE 18, HITECH, and PCI 4.0. Our service will help you maintain the necessary controls, documentation, and audit trails to demonstrate compliance and mitigate the risk of non-compliance penalties.

24x7 Incident Response and Remediation: If you have purchased our security service, in the event of a security incident arising our 24/7 Security Operations Centre team provides comprehensive incident response and remediation services. We will work with your team and partners to contain the breach, investigate the root cause, and implement appropriate measures to prevent similar incidents from occurring in the future.

Ongoing Support and Optimisation: Our service includes regular reviews, updates, and optimisation of your PeopleSoft security measures. We will keep you informed of the latest security threats, industry best practices, and Oracle security updates, ensuring your Oracle systems remain secure and up to date.

The Support Revolution Security Team analyse all vulnerabilities announced by Oracle and grade them based on the severity of the vulnerability and the likelihood of information being available to allow an attacker to exploit it. They then inform your team of actions to take to protect your systems.

By partnering with us for your Oracle Security Hardening, Monitoring, and Protection Service, you can rest assured that your critical Oracle systems are in safe hands. Our expertise, cutting-edge technology, and commitment to your security will help you navigate the ever-evolving cybersecurity landscape and protect your organisation's most valuable assets.

We provide a range of additional bespoke fee-based security services including:

- In-depth security assessments to evaluate the security posture of your estate and provide guidance on improving security within your processes and infrastructure.
- Implementing additional security solutions, tools and compensating controls.
- Advice and guidance on your security roadmap.

We are ISO9001 (quality), ISO27001 (security) and Cyber Essentials accredited.

2.8 Service Management & Reporting

(a) Service Management

Exhibit A

The Head of our PeopleSoft Practice hand-picks the Primary Support Engineer that will oversee the delivery of our service to you based on their technical and industry knowledge, location and expertise. Your Primary Support Engineer then hand-picks the team that will support you based on your technical and geographical support needs, with local teams in your regions backed up by our full global team.

We will provide you with an Account Management team who will oversee the quality of the service provided to you. We will ask you to appoint a lead representative to attend support meetings. These are conference calls with our Service Desk Manager, usually 30 minutes long during which we review all open incidents, agree actions, next steps, and priorities. The frequency of these calls will depend on the volume of incidents raised.

In addition, we provide monthly Service Review meetings via video link with your team to review our service, any complex support cases and key performance against the SLA.

Quarterly Review meetings will be scheduled to review progress over the past three months. These meetings are an opportunity to discuss any upcoming plans and additional support needs or changes in scope, including any service improvements.

The table below provides a summary of our service reporting:

TYPE OF COMMUNICATION	SUPPORT REVOLUTION CONTACT	SCOPE OF COMMUNICATION
Support Calls Weekly / Bi-Weekly / Monthly	Service Desk Manager	Review all open incidents, agree actions and next steps and priorities Review open Change Requests and progress
Service Review Monthly	Support Manager	Review Monthly Service Reports, open and closed cases and performance against the SLA Review open Change Requests
Quarterly Reviews	Head of Support Services Primary Support Engineer	Review progress over past three months Discuss any upcoming plans and additional support needs or changes in scope Discuss service improvements
Quarterly Account Manager Reviews	Head of Account Management	Non-technical review of the support service and governance of the support contract to ensure that you are you happy with the service

As part of our standard reporting, we provide automated service reports via our support portal that contain the following information:

- Incidents opened last month
- Incidents opened this month
- Incidents closed last month
- Incidents opened last month by category and age
- SLA performance last month
- SLA performance last 12 months
- Incidents closed last 12 months by month
- Incidents opened last 12 months by category
- Service requests raised
- Open change requests by status with estimates
- Open problems by category
- Closed problems by category / priority

You can drill down on any report to the data beneath it and see all actions taken by time and date on any incident, problem, service request or change.

2.9 Transitioning To Our Service

Exhibit A

During the transition to Support Revolution, we will meet with your team to discuss and understand the PeopleSoft environment in detail. This will help us understand your future plans for IT software upgrades, hardware refreshes and determine potential upgrade paths. We will use this information to download any Oracle software which you are entitled to and may need in the future.

We will supply your team with the Support Revolution PeopleSoft Questionnaire that needs to be completed by your support staff. This will provide us with the technical details regarding your current software versions.

2.10 Additional Benefits

Our service includes a range of additional benefits:

- **Revolutionary SLA.** We offer guaranteed Resolution Times for incidents, demonstrating how committed we are to resolving your issues in a timely manner.
- **Revolutionary Security.** For an additional cost, we will implement and train your team how to use Trend Micro Deep Security to replace and improve upon the security of your Oracle systems. We then provide advice and guidance on security hardening for your systems and provide ongoing advice and guidance as new security threats evolve.
- **Revolutionary License Advisory.** We assist you to optimise your Oracle licenses and how these are deployed across your estate within our service. Should you be audited by Oracle, we offer full support to you during the audit.

Exhibit A

3. Appendix A - Service Level Agreement

The standard Support Revolution contract includes a detailed Service Level Agreement (SLA).
Each Incident reported to the Service Desk is allocated an Impact (High, Medium or Low) and an Urgency (High, Medium or Low) in line with ITIL best practice. The Impact and Urgency of an Incident is used to determine its Priority, as follows:

Impact	Urgency	Priority
High	High	1
High	Medium	2
Medium	High	2
Medium	Medium	3
Medium	Low	4
Low	Medium	4
Low	Low	5

Our standard SLA includes the following Initial Response Commitments, Client Update Commitments and Target Resolution Times:

PRIORITY	INITIAL RESPONSE COMMITMENT	CLIENT UPDATE COMMITMENT	TARGET RESOLUTION TIME
1	10 Elapsed Minutes	Every 1 Elapsed Hour	2 hours
2	20 Elapsed Minutes	Every 1 Business Hour	4 hours
3	4 Elapsed Hours	Every 1 Business Day	3 days
4	1 Business Day	As appropriate	5 days
5	1 Business Day	As appropriate	10 days

A description of the types of Incidents that typically fall within each Priority is set out in **Table A**, below:

Exhibit A

SERVICE LEVELS

PRIORITY	DEFINITION	RESPONSE SERVICE LEVEL	RESOLUTION SERVICE LEVEL
1	• Significant adverse impact on service to a large number of end users • Causes significant financial loss and/or disruption • Results in any material loss or corruption of data • Significant security threat to Client's business • May have a damaging effect on Client reputation	**Service Level Performance Measure** 100% within 10 minutes **Service Level Threshold** 100% within 30 minutes	**Service Level Performance Measure** 90% within 2 hours **Service Level Threshold** 90% within one business day
2	• Has a moderate adverse impact on the delivery of service to a large number of end users • Causes a loss and/or disruption to The Client which is more than trivial but less severe than the significant financial loss described in the definition of a severity 1 incident	**Service Level Performance Measure** 100% within 20 minutes **Service Level Threshold** 100% within 2 hours	**Service Level Performance Measure** 90% within 4 hours **Service Level Threshold** 90% within two business days
3	• Has a moderate adverse impact upon the delivery of service to a small (i.e. 1 or more) or moderate number of end users	**Service Level Performance Measure** 100% within 4 hours **Service Level Threshold** 100% within 1 business day	**Service Level Performance Measure** 90% within 3 business days **Service Level Threshold** 90% within 5 business days
4	• Has a minor adverse impact upon the delivery of service to a small number of end users	**Service Level Performance Measure** 100% within 8 hours **Service Level Threshold** 100% within 2 business days	**Service Level Performance Measure** 90% within 5 business days **Service Level Threshold** 90% within 7 business days
5	• Has minimal or no impact upon the delivery of service	**Service Level Performance Measure** 100% within 3 business days **Service Level Threshold** 100% within 5 business days	**Service Level Performance Measure** 90% < 10 business days **Service Level Threshold** 90% < 20 business days

In the table above:

- **"Response Service Level"** is the time within which we need to respond to an incident.
- **"Resolution Service Level"** is the time within which we need to resolve the incident.

- **"Service Level Performance Measure" (SPM)** is the percentage of incidents to be responded to / resolved within a certain time.
- **"Service Level Threshold" (SLT)** is a less ambitious target than the Service Level Performance Measure and represents the maximum time expected even under exceptional circumstances.

As can be seen in the table above, for a Priority 1 incident, the SLA includes the following response targets:

- **Service Level Performance Measure**
- 100% within 10 minutes
- **Service Level Threshold**
- 100% within 30 minutes

The above states that we need to respond to all Priority 1 incidents within 10 minutes or we will have missed the target. Further, if we have failed to meet this target and then not respond within 30 minutes, we will have missed the Service Level Threshold.

Exhibit B

Amendment to
Third Party Support Services Agreement

This amendment ("**Amendment One**") amends the Third Party Support Services Agreement dated [DATE] (the "**Agreement**") by and between Support Revolution, Inc., a Delaware corporation, whose office is at 111 Congress, Suite 500, Austin Texas (the "**Supplier**") and [CUSTOMER NAME], a [ENTITY TYPE], whose office is at [ADDRESS] (the "**Client**").

WHEREAS, pursuant to the terms of the Agreement, Client has engaged Supplier to provide Services connected to Oracle Corporation's ("**Oracle**") PeopleSoft suite of products ("**PeopleSoft**");

WHEREAS, prior to the execution of the Agreement, Rimini Street, Inc. ("**Rimini Street**") was providing Client with third party support services for PeopleSoft;

WHEREAS, at the time of the execution of this Agreement, Rimini Street is involved in at least two concurrent litigations with Oracle regarding, among other things, Rimini Street's provision of third party support services for PeopleSoft, including *Oracle USA, Inc. v. Rimini Street*, Case No. 2:10-cv-00106-LRH-VCF (D. Nev. Filed Jan. 25, 2010) (hereinafter "***Rimini I***") and *Oracle International Corporation v. Rimini Street*, Case No. 2:14-cv-1699-MMD-DJA (D. Nev. Filed October 15, 2014) ("***Rimini II***");

WHEREAS, at the time of the execution of this Agreement, Rimini Street is subject to at least two permanent injunctions that, in part, enjoin Rimini Street from certain actions in connection with the provision of third party support services for PeopleSoft, including Document 1166, filed August 15, 2018 in *Rimini I,* and Document 1537, filed July 24, 2023 in *Rimini II*;

WHEREAS, at the time of the execution of this Agreement, Client represents and warrants that it has not received and has no knowledge of any claim by a Third Party, including but not limited to Oracle Corporation, containing an express or implied allegation that Client is or may be infringing the Intellectual Property Rights of a Third Party as a result of Rimini Street's provision to Client of third party support services for PeopleSoft;

WHEREAS, in light of the proceedings in *Rimini I* and *Rimini II*, which are ongoing and subject to change, Client and Supplier wish to amend and augment the Agreement in order to: (1) expand the scope of work; and (2) clarify and/or put in place additional warranties and liability limitations, as set forth below;

NOW THEREFORE, in consideration of the representations and agreements contained in this Amendment One and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Client and Supplier agree to amend and augment the Agreement as follows:

1. REMOVAL OF RIMINI STREET CODE

Client and Supplier agree to put in place a process by which any and all source and object code created, written, copied, inserted, or otherwise provided by Rimini Street ("Rimini Street Code") is eliminated from the Client's Systems. Towards that end, within 60 days of execution of the Agreement, Supplier will review Client's Systems and prepare a provisional plan for the removal of Rimini Street Code ("**Provisional Removal Plan**"). The Provisional Removal Plan will identify, at a minimum, the following: (a) the specific tasks that must be completed in order to identify and remove Rimini Street Code; (b) assignment of tasks in (a) above to either Client or Supplier; (c) the anticipated timeline for the completion of the tasks identified in (a) above; and (d) estimated cost to the Client for completing the Removal Plan. Supplier will review the Provisional Removal Plan with Client and give Client the opportunity to provide input regarding the same. Within 30 days of the delivery of the Provisional Removal Plan, Client and Supplier will agree to the final terms of the plan for the removal of Rimini Street Code ("**Final Removal Plan**"). The Final Removal Plan must be executed by both Client and Supplier and the terms of the Final Removal Plan will be integrated into this Amendment as if fully stated herein.

2. CLIENT WARRANTY REGARDING NON-DISCLOSURE OF RIMINI STREET MATERIALS AND INFORMATION

Client warrants that it has not and, further, will not disclose to Supplier, in written or oral form, anything provided or disclosed to the Client by Rimini Street in connection with the provisions of PeopleSoft third party support services. This includes, at a minimum, contractual materials, agreements, strategies, plans, processes, reports, scope, timelines, benchmarking and anything related to the forgoing. In the event that Client discloses anything to Supplier in contravention of this provision, Supplier will have the right to terminate the Agreement at its sole discretion. In the event of such termination, any fees paid by Client to Supplier shall be non-refundable.

3. NO SUPPLIER WARRANTY REGARDING LIABILITY TO ORACLE

Client and Supplier acknowledge and agree that the warranties contained in Section 17 of the Agreement apply to this Amendment and otherwise remain in force and effect. For the sake of clarity, Client further acknowledges and agrees that Supplier expressly does not represent or warrant that execution of the Final Removal Plan will result in Client being free from retroactive or prospective liability to Oracle related to or in connection with Rimini Street's provision to Client of third party support services for PeopleSoft. In an abundance of clarity, Client further acknowledges and agrees that Client bears sole responsibility to Oracle for any liability related to or in connection with Rimini Street's provision to Client of third party support services for PeopleSoft.

4. LIMITATION OF LIABILITY AND INDEMNITY

In addition to the limitations of liability contained in Section 18 of the Agreement, Client acknowledges and agrees that Supplier shall have no liability to Client related to or in connection with Rimini Street's provision to Client of third party support services for PeopleSoft. Further, Client agrees to indemnify Supplier against any claims made by Oracle against Supplier that are related to or in connection with Rimini Street's provision to Client of third party support services for PeopleSoft.

Exhibit B

5. ORDER OF PRECEDENCE

Client and Supplier agree that the terms of this Amendment One will prevail in the event of any inconsistencies with any terms of the Agreement.

Other than the changes above, the terms and conditions of the Agreement unchanged and in full force and effect.

* * *

This Agreement has been signed by a duly authorized representative of each party on the date appearing below.

Signed for and on behalf of [CLIENT]	**Signed for and on behalf of Support Revolution Limited**
Signature:	DocuSigned by: Signature Victoria Molloy AD54347AAFF7475...
Name: Nathan Magsig	Name: Victoria Molloy
Title:Chairman of the Board of Supervisors of the County of Fresno	Title: Chief Commercial Officer
Date: 12/17/2024	Date: 18-Nov-24 | 12:50 AM PST

Attest:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: ____________
Deputy

Exhibit C

A. Definitions.

Capitalized terms used in this Exhibit C have the meanings set forth in this section A.

"Authorized Employees" means the Contractor's employees who have access to Personal Information.

"Authorized Persons" means: (i) any and all Authorized Employees; and (ii) any and all of the Contractor's subcontractors, representatives, agents, outsourcers, and consultants, and providers of professional services to the Contractor, who have access to Personal Information and are bound by law or in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms of this Exhibit C.

"Director" means the County's Director of Internal Services/Chief Information Officer or his or her designee.

"Disclose" or any derivative of that word means to disclose, release, transfer, disseminate, or otherwise provide access to or communicate all or any part of any Personal Information orally, in writing, or by electronic or any other means to any person.

"Person" means any natural person, corporation, partnership, limited liability company, firm, or association.

"Personal Information" means any and all information, including any data provided, or to which access is provided, to the Contractor by or upon the authorization of the County, including but not limited to vital records, that: (i) identifies, describes, or relates to, or is associated with, or is capable of being used to identify, describe, or relate to, or associate with, a person (including, without limitation, names, physical descriptions, signatures, addresses, telephone numbers, e-mail addresses, education, financial matters, employment history, and other unique identifiers, as well as statements made by or attributable to the person); (ii) is used or is capable of being used to authenticate a person (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or personal identification numbers (PINs), financial account numbers, credit report information, answers to security questions, and other personal identifiers); or is personal information within the meaning of California Civil Code section 1798.3, subdivision (a), or 1798.80, subdivision (e). Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Privacy Practices Complaint" means a complaint received by the County relating to the Contractor's (or any Authorized Person's) privacy practices, or alleging a Security Breach. Such complaint shall have sufficient detail to enable the Contractor to promptly investigate and take remedial action under this Exhibit C.

"Security Safeguards" means physical, technical, administrative or organizational security procedures and practices put in place by the Contractor (or any Authorized Persons) that relate to the protection of the security, confidentiality, value, or integrity of Personal Information. Security Safeguards shall satisfy the minimal requirements set forth in subsection C.(5) of this Exhibit C.

"Security Breach" means (i) any act or omission that compromises either the security, confidentiality, value, or integrity of any Personal Information or the Security Safeguards, or (ii) any unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, any Personal Information.

"Use" or any derivative thereof means to receive, acquire, collect, apply, manipulate, employ, process, transmit, disseminate, access, store, disclose, or dispose of Personal Information.

B. Standard of Care.

(1) The Contractor acknowledges that, in the course of its engagement by the County under this Agreement, the Contractor, or any Authorized Persons, may Use Personal Information only as permitted in this Agreement.

(2) The Contractor acknowledges that Personal Information is deemed to be confidential information of, or owned by, the County (or persons from whom the County receives or has received Personal Information) and is not confidential information of, or owned or by, the Contractor, or any Authorized Persons. The Contractor further acknowledges that all right, title, and interest in or to the Personal Information remains in the County (or persons from whom the County receives or has received Personal Information) regardless of the Contractor's, or any Authorized Person's, Use of that Personal Information.

(3) The Contractor agrees and covenants in favor of the County that the Contractor shall: (i) keep and maintain all Personal Information in strict confidence, using such degree of care under this Subsection B as is reasonable and appropriate to avoid a Security Breach; (ii) Use Personal Information exclusively for the purposes for which the Personal Information is made accessible to the Contractor pursuant to the terms of this Exhibit C; (iii) not Use, Disclose, sell, rent, license, or otherwise make available Personal Information for the Contractor's own purposes or for the benefit of anyone other than the County, without the County's express prior written consent, which the County may give or withhold in its sole and absolute discretion; and (iv) not, directly or indirectly, Disclose Personal Information to any person (an "Unauthorized Third Party") other than Authorized Persons pursuant to this Agreement, without the Director's express prior written consent.

Notwithstanding the foregoing paragraph, in any case in which the Contractor believes it, or any Authorized Person, is required to disclose Personal Information to government regulatory authorities, or pursuant to a legal proceeding, or otherwise as may be required by applicable law, the Contractor shall (a) immediately notify the County of the specific demand for, and legal authority for the disclosure, including providing the County with a copy of any notice, discovery demand, subpoena, or order, as applicable, received by the Contractor, or any Authorized Person, from any government regulatory authorities, or in relation to any legal proceeding, and (b) promptly notify the County before such Personal Information is offered by the Contractor for such disclosure so that the County may have sufficient time to obtain a court order or take any other action the County may deem necessary to protect the Personal Information from such disclosure, and the Contractor shall cooperate with the County to minimize the scope of such disclosure of such Personal Information.

The Contractor shall remain liable to the County for the actions and omissions of any Unauthorized Third Party concerning its Use of such Personal Information as if they were the Contractor's own actions and omissions.

C. Information Security.

(1) The Contractor covenants, represents and warrants to the County that the Contractor's Use of Personal Information under this Agreement does and shall at all times comply with all federal, state, and local, privacy and data protection laws, as well as all other applicable regulations and directives, including but not limited to California Civil Code, Division 3, Part 4, Title 1.81 (beginning with section 1798.80), and the Song-Beverly Credit Card Act of 1971 (California Civil Code, Division 3, Part 4, Title 1.3, beginning with section 1747). If the Contractor Uses credit, debit, or other payment cardholder information, the Contractor shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing and maintaining all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the Contractor's sole cost and expense.

(2) The Contractor covenants, represents and warrants to the County that, as of the Effective Date, the Contractor has not received notice of any violation of any privacy or data protection laws, as well as any other applicable regulations or directives, and is not the subject of any pending legal action or investigation by, any government regulatory authority regarding same.

(3) Without limiting the Contractor's obligations under subsection C.(1) of this Exhibit C, the Contractor's (or Authorized

Exhibit C

Person's) Security Safeguards shall be no less rigorous than accepted industry practices and, at a minimum, include the following: (i) limiting Use of Personal Information strictly to the Contractor's and Authorized Persons' technical and administrative personnel who are necessary for the Contractor's, or Authorized Persons', Use of the Personal Information pursuant to this Agreement; (ii) ensuring that all of the Contractor's connectivity to the County computing systems will only be through the County's security gateways and firewalls, and only through security procedures approved upon the express prior written consent of the Director; (iii) to the extent that they contain or provide access to Personal Information, (a) securing the Contractor's business facilities, data centers, paper files, servers, back-up systems and computing equipment, operating systems, and software applications, including, but not limited to, all mobile devices and other equipment, operating systems, and software applications with information storage capability; (b) employing adequate controls and data security measures with respect to the Contractor Facilities and Equipment), both internally and externally, to protect (1) the Personal Information from potential loss or misappropriation, or unauthorized Use, and (2) the County's operations from disruption and abuse; (c) having and maintaining network, device application, database and platform security; (d) maintaining authentication and access controls within media, computing equipment, operating systems, and software applications; and (e) installing and maintaining in all mobile, wireless, or handheld devices a secure internet connection, having continuously updated anti-virus software protection and a remote wipe feature always enabled, all of which is subject to express prior written consent of the Director; (iv) encrypting all Personal Information at advance encryption standards of Advanced Encryption Standards (AES) of 128 bit or higher (a) stored on any mobile devices, including but not limited to hard disks, portable storage devices, or remote installation, or (b) transmitted over public or wireless networks (the encrypted Personal Information must be subject to password or pass phrase, and be stored on a secure server and transferred by means of a Virtual Private Network (VPN) connection, or another type of secure connection, all of which is subject to express prior written consent of the Director); (v) strictly segregating Personal Information from all other information of the Contractor, including any Authorized Person, or anyone with whom the Contractor or any Authorized Person deals so that Personal Information is not commingled with any other types of information; (vi) having a patch management process including installation of all operating system/software vendor security patches; (vii) maintaining appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks of Authorized Employees consistent with applicable law; and (viii) providing appropriate privacy and information security training to Authorized Employees.

(4) During the term of each Authorized Employee's employment by the Contractor, the Contractor shall cause such Authorized Employees to abide strictly by the Contractor's obligations under this Exhibit C. The Contractor further agrees that it shall maintain a disciplinary process to address any unauthorized Use of Personal Information by any Authorized Employees.

(5) The Contractor shall, in a secure manner, backup daily, or more frequently if it is the Contractor's practice to do so more frequently, Personal Information received from the County, and the County shall have immediate, real time access, at all times, to such backups via a secure, remote access connection provided by the Contractor, through the Internet.

(6) The Contractor shall provide the County with the name and contact information for each Authorized Employee (including such Authorized Employee's work shift, and at least one alternate Authorized Employee for each Authorized Employee during such work shift) who shall serve as the County's primary security contact with the Contractor and shall be available to assist the County 24 hours per day, seven days per week as a contact in resolving the Contractor's and any Authorized Persons' obligations associated with a Security Breach or a Privacy Practices Complaint.

D. Security Breach Procedures.

(1) Promptly, and without undue delay, upon the Contractor's confirmation of a Security Breach, the Contractor shall (a) notify the Director of the Security Breach, such notice to be given first by telephone at the following telephone number, followed promptly by email at the following email address: (559) 600-5900 / incidents@fresnocountyca.gov (which telephone number and email address the County may update by providing notice to the Contractor), and (b) preserve all relevant evidence (and cause any affected Authorized Person to preserve all relevant evidence) relating to the Security Breach. The notification shall include, to the extent reasonably possible, the identification of each type and the extent of Personal Information that has been, or is reasonably believed to have been, breached, including but not limited to, compromised, or subjected to unauthorized Use, Disclosure, or modification, or any loss or destruction, corruption, or damage.

(2) Immediately following the Contractor's notification to the County of a Security Breach, as provided pursuant to subsection D.(1) of this Exhibit C, the Parties shall coordinate with each other to investigate the Security Breach. The Contractor agrees to fully cooperate with the County, including, without limitation: (i) assisting the County in conducting any investigation; (ii) providing the County with physical access to the facilities and operations affected; (iii) facilitating interviews with Authorized Persons and any of the Contractor's other employees knowledgeable of the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the County. To that end, the Contractor shall, with respect to a Security Breach, be solely responsible, at its cost, for all notifications required by law and regulation, and the Contractor shall provide a written report of the investigation and reporting required to the Director within 30 days after the Contractor's discovery of the Security Breach.

(3) The County shall promptly notify the Contractor of the Director's knowledge, or reasonable belief, of any Privacy Practices Complaint, and upon the Contractor's receipt of notification thereof, the Contractor shall promptly address such Privacy Practices Complaint, including taking any corrective action under this Exhibit C, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. In the event the Contractor discovers a Security Breach, the Contractor shall treat the Privacy Practices Complaint as a Security Breach. Within 24 hours of the Contractor's receipt of notification of such Privacy Practices Complaint, the Contractor shall notify the County whether the matter is a Security Breach, or otherwise has been corrected and the manner of correction, or determined not to require corrective action and the reason therefor.

(4) The Contractor shall take prompt corrective action to respond to and remedy any Security Breach and take reasonable mitigating actions, including but not limiting to, preventing any reoccurrence of the Security Breach and correcting any deficiency in Security Safeguards as a result of such incident, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. The Contractor shall reimburse the County for all reasonable costs incurred by the County in responding to, and mitigating damages caused by, any Security Breach, including all costs of the County incurred in relation to any litigation or other action described in subsection D.(5) of this Exhibit C to the extent applicable: (1) the cost of providing affected individuals with credit monitoring services for a specific period not to exceed 12 months, to the extent the incident could lead to a compromise of the data subject's credit or credit standing; (2) call center support for such affected individuals for a specific period not to exceed 30 days; and (3) the cost of any measures required under applicable laws.

E. Oversight of Security Compliance.

(1) The Contractor shall have and maintain a written information security policy that specifies Security Safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

(2) Upon the County's written request, to confirm the Contractor's compliance with this Exhibit C, as well as any applicable laws, regulations and industry standards, the Contractor grants the County or, upon the County's election, a third party on the County's behalf, permission to perform an assessment, audit, examination or review of all controls in the Contractor's physical and technical environment in relation to all Personal Information that is Used by the Contractor pursuant to this Agreement. The Contractor shall fully cooperate with such assessment, audit or examination, as applicable, by providing the County or the third party on the County's behalf, access to all Authorized Employees and other knowledgeable personnel, physical premises, documentation, infrastructure and application software that is Used by the Contractor for Personal Information pursuant to this Agreement. In addition, the Contractor shall provide the County with the results of any audit by or on behalf of the Contractor that assesses the effectiveness of the Contractor's information security program as relevant to the security and confidentiality of Personal Information Used by the Contractor or Authorized Persons during the course of this Agreement under this Exhibit C.

(3) The Contractor shall ensure that all Authorized Persons who Use Personal Information agree to the same restrictions and conditions in this Exhibit C. that apply to the Contractor with respect to such Personal Information by incorporating the relevant provisions of these provisions into a valid and binding written agreement between the Contractor and such Authorized Persons, or amending any written agreements to provide same.

F. Return or Destruction of Personal Information.

Upon the termination of this Agreement, the Contractor shall, and shall instruct all Authorized Persons to, promptly return to the County all Personal Information, whether in written, electronic or other form or media, in its possession or the possession of such Authorized Persons, in a machine readable form used by the County at the time of such return, or upon the express prior written consent of the Director, securely destroy all such Personal Information, and certify in writing to the County that such Personal Information have been returned to the County or disposed of securely, as applicable. If the Contractor is authorized to dispose of any such Personal Information, as provided in this Exhibit C, such certification shall state the date, time, and manner (including standard) of disposal and by whom, specifying the title of the individual. The Contractor shall comply with all reasonable directions provided by the Director with respect to the return or disposal of Personal Information and copies thereof. If return or disposal of such Personal Information or copies of Personal Information is not feasible, the Contractor shall notify the County accordingly, specifying the reason, and continue to extend the protections of this Exhibit C to all such Personal Information and copies of Personal Information. The Contractor shall not retain any copy of any Personal Information after returning or disposing of Personal Information as required by this section F. The Contractor's obligations under this section F survive the termination of this Agreement and apply to all Personal Information that the Contractor retains if return or disposal is not feasible and to all Personal Information that the Contractor may later discover.

G. Equitable Relief.

The Contractor acknowledges that any breach of its covenants or obligations set forth in this Exhibit C may cause the County irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the County is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the County may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available to the County at law or in equity or under this Agreement.

H. Indemnification.

The Contractor shall defend, indemnify and hold harmless the County, its officers, employees, and agents, (each, a **"County Indemnitee"**) from and against any and all infringement of intellectual property including, but not limited to infringement of copyright, trademark, and trade dress, invasion of privacy, information theft, and extortion, unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, Personal Information, Security Breach response and remedy costs, credit monitoring expenses, forfeitures, losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, fines, and penalties (including regulatory fines and penalties), costs or expenses of whatever kind, including attorney's fees and costs, the cost of enforcing any right to indemnification or defense under the Agreement and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim or action against any County Indemnitee in relation to the Contractor's, its officers, employees, or agents, or any Authorized Employee's or Authorized Person's, performance or failure to perform under this Exhibit C or arising out of or resulting from the Contractor's failure to comply with any of its obligations under this section H. The provisions of this section H do not apply to the acts or omissions of the County. The provisions of this section H are cumulative to any other obligation of the Contractor to, defend, indemnify, or hold harmless any County Indemnity under this Agreement. The provisions of this section H shall survive the termination of this Agreement.

I. Survival.

The respective rights and obligations of the Contractor and the County as stated in this Exhibit C shall survive the termination of this Agreement.

J. No Third Party Beneficiary.

Nothing express or implied in the provisions of in this Exhibit C is intended to confer, nor shall anything herein confer, upon any person other than the County or the Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

L. No County Warranty.

The County does not make any warranty or representation whether any Personal Information in the Contractor's (or any Authorized Person's) possession or control, or Use by the Contractor (or any Authorized Person), pursuant to the terms of this Agreement is or will be secure from unauthorized Use, or a Security Breach or Privacy Practices Complaint.

Exhibit D

Self-Dealing Transaction Disclosure Form

In order to conduct business with the County of Fresno ("County"), members of a contractor's board of directors ("County Contractor"), must disclose any self-dealing transactions that they are a party to while providing goods, performing services, or both for the County. A self-dealing transaction is defined below:

> "A self-dealing transaction means a transaction to which the corporation is a party and in which one or more of its directors has a material financial interest."

The definition above will be used for purposes of completing this disclosure form.

Instructions

(1) Enter board member's name, job title (if applicable), and date this disclosure is being made.

(2) Enter the board member's company/agency name and address.

(3) Describe in detail the nature of the self-dealing transaction that is being disclosed to the County. At a minimum, include a description of the following:

a. The name of the agency/company with which the corporation has the transaction; and

b. The nature of the material financial interest in the Corporation's transaction that the board member has.

(4) Describe in detail why the self-dealing transaction is appropriate based on applicable provisions of the Corporations Code.

The form must be signed by the board member that is involved in the self-dealing transaction described in Sections (3) and (4).

Exhibit D

(1) Company Board Member Information:			
Name:		**Date:**	
Job Title:			
(2) Company/Agency Name and Address:			
(3) Disclosure (Please describe the nature of the self-dealing transaction you are a party to)			
(4) Explain why this self-dealing transaction is consistent with the requirements of Corporations Code § 5233 (a)			
(5) Authorized Signature			
Signature:		Date:	