MASTER SAAS & SERVICES AGREEMENT

This Master SaaS and Services Agreement ("**Agreement**") is entered into to be effective as of the date of later signature below ("**Effective Date**") between iOFFICE, LP with its wholly owned subsidiaries: Hippo Facility Management Technologies, Inc., Teem Technologies, LLC, and ManagerPlus Solutions, LP ("**Company**"), and the Customer executing this Agreement ("**Customer**") (together the "**Parties**") and approved by the City Attorney in accordance with Charter section 40. This Agreement establishes the basic terms of the relationship between the Parties for the Service and Professional Services provided by Company. To establish the mutual promises set out in this Agreement and for other good and valuable consideration, Company and Customer agree as follows:

1. **Definitions.**

"**Affiliates**" means any entity which directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with a Party to this Agreement (whether by way of majority voting stock ownership or the ability to otherwise direct or cause the direction of the management and policies of such party, for so long as such control exists).

"Applications" means the software applications set forth in the Scope of Work ("SOW") or otherwise made available by Company for use by Customer under the terms of this Agreement.

"**Confidential Information**" means, except as set forth herein: (a) Customer Data; (b) the terms of this Agreement; and (c) any commercial, financial, marketing, business, technical or other data, security measures and procedures, know-how or other information disclosed by or on behalf of the disclosing party to the receiving party for purposes arising out of or in connection with this Agreement, that: (i) in the case of information in tangible form, is marked "confidential" or "proprietary;" and (ii) information that under the circumstances, a person exercising reasonable business judgment would understand to be confidential or proprietary; Notwithstanding the foregoing, the following shall not be Confidential Information: (1) information that was in the public domain at the time of its disclosure, or which becomes public domain property through no fault of the receiving party (2) information that was rightfully in the receiving party's possession without restriction prior to disclosure; (3) information that was rightfully disclosed to the receiving party by a third-party without restriction and (4) information that was independently developed by employees and/or contractors of the receiving party who did not have access to and without use of or reference to the disclosing party's Confidential Information.
"**Customer Data**" means all electronic data or information submitted to and stored in the Service by Customer and its Users. Personal data may include (a) Personal Information as defined within the CCPA or GDPR; (b) identifies an individual, including by name, email address, telephone number; and (c) pertains to an individual's medical history, physical condition, or medical treatment.

"**DPA**" means the Company's Data Processing Agreement which regulates the particularities of data processing.

"Documentation" means on-line or hardcopy, help, guides, and manuals published online by Company that relate to the use of the Applications and/or Services that have been provided to Customer.

"**Hardware**" means the sensors and accessories designed, developed, and manufactured by VergeSense, including any software included therein, that are a part of the services (if purchased by Customer) provided by Company.

"**Order Form**" means a Company provided quote or order form in the name of and executed by Customer or its Affiliate and accepted by Company which specifies the Service, term of license to use the Service, and payment details to be provided by Company subject to the terms of this Agreement (incorporated by reference and/or attached as Exhibit A).

"**Professional Services**" means the general consulting, implementation or training professional services to be provided to Customer pursuant to a related Statement of Work ("SOW") or included in the Customer's Order Form.

"Reports" means any reports that incorporate Customer Data generated by or through the Services or Company proprietary software, or for the benefit of, Customer.

"**Service**" means, collectively, the Company software and products being provided to Customer on a software-as-a-service (SaaS) basis and certain software applications, as further set forth on an Order Form.

“**Support Services**” means the technical support services to be provided to Customer pursuant to the support policy terms found at the following (or such other URL as specified by Company from time to time), incorporated herein by reference, (“**Service Level Agreement (SLA)**”): *(applicable link depends on which Company products purchased)*

Hippo Facility Management Technologies, Inc.: https://www.hippocmms.com/agreement-service-level
iOFFICE, LP: https://www.iofficecorp.com/sla
ManagerPlus Solutions, LP: https://www.managerplus.com/sla
Teem Technologies, LLC: https://www.teem.com/service-level-agreement-sla/

“**Third-Party Applications**” means applications, integrations, services, or implementation, customization and other consulting services related thereto, provided by a party other than Company that interoperate with the Service, including but not limited to those listed in the help Documentation.

“Updates” shall mean (a) subsequent releases of the Applications that (i) add new features, functionality, and/or improved performance, (ii) operate on new or other databases, operating systems, or client or server platforms, or (iii) add new foreign language capabilities; and (b) bug or error fixes, patches, workarounds, and maintenance releases.

“**Users**” means individuals who are authorized by Customer or its Affiliate to use the Service pursuant to the Agreement or as otherwise defined, restricted or limited in an Order Form or amendment, for whom subscriptions to a Service have been procured. Users include but are not limited to Customer and Customer’s Affiliates’ employees, consultants, contractors, and agents.

2. **Use of Service**.

a. **Term.** This Agreement will remain in effect until Customer’s subscription and/or license to use the Services expires according to the term on the Customer’s Order Form or if the Agreement is terminated for reasons herein. Company may charge automatically at the end of the initial and/or each term for the renewal, unless Customer notifies Company in writing that the Customer wants to cancel or disable autorenewal thirty (30) days prior to the same taking effect. In no event shall the term of this agreement exceed five (5) years.

b. **Right of Use**. Company grants to Customer a non-exclusive, worldwide, and non-transferable license to use the Service during the initial Term and any subsequent Renewal Term(s) according to the Customer’s Order Form. The Customer may only use the Services for Customer’s internal business purposes. The Agreement does not contemplate any customized work or coding work developed specifically for Customer.

c. **Customer Responsibilities**. Customer shall be responsible at all times for: (a) all activity generated by it or its Users; (b) ensuring compliance with this Agreement by it and each User; and (c) ensuring compliance with applicable local, state, national, and foreign laws, treaties, and regulations in connection with your use of the Service, including those related to data privacy and the transmission of data.

d. **Changes to Services**. Company may, in its sole discretion, make any changes to any Service that it deems necessary or useful only to (i) maintain or enhance (a) the quality or delivery of Company’s products or services to its customers, (b) the competitive strength of, or market for, Company’s products or services or (ii) to comply with applicable law. Company shall not degrade performance of the Service in the event of any changes.

e. **General Restrictions**. Customer must not use, and must ensure that Affiliates do not rent, resell, or sublicense the Service. Customer shall not and shall not permit any Affiliate, or User to: (a) copy, translate, create a derivative work of, reverse engineer, reverse assemble, disassemble, or decompile the Service or any part thereof or otherwise attempt to discover any source code or modify the Service in any manner or form unless expressly allowed in the help Documentation; (b) use the Service for the purpose of building a similar or competitive product or service, or (c) publish, post, upload or otherwise transmit Customer Data that contains any viruses, Trojan horses, worms, time bombs, corrupted files or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any systems, data, personal information or property of another.

f. **Third-Party Applications (if applicable)**. Company or third-party providers may offer Third-Party Applications. Except as expressly set forth in the Order Form, Company does not warrant any such Third-Party Applications, regardless of whether or not such Third-Party Applications are provided by a third-party that is a member of a Company partner program or otherwise designated by Company as “built for”, "certified," "approved" or “recommended.” Any procurement by Customer of such Third-Party Applications or services is solely between Customer and the applicable third-party provider. If Customer installs or enables Third-Party Applications for use with the Service, Customer agrees that Company may enable such third-party providers to access Customer Data for the interoperation of such Third-Party Applications with the Service, and any exchange of data or other interaction between Customer and a third-party provider is solely between Customer and such third-party provider pursuant to a separate privacy policy or other terms governing Customer’s access to or use of the Third-Party Applications. Company shall not be responsible for any disclosure, modification or deletion of Customer Data resulting from any such access by Third-Party Applications or third-party providers. No procurement of such Third-Party Applications is required to use the Service.

g. **Subscription Services**. Each applicable Order Form shall specify the Services to be provided and shall identify each applicable Application.

h. **Support Services**. As part of the Service, Company will provide Customer with the level of Support Services as further set forth in the SLA. Company does not provide Support Services for problems that are caused by the Hardware. In the event Customer experiences Hardware issues (e.g. battery replacements, sensor reboots, gateway reboots, sensor replacements), Customer must contact support@vergesense.com.

i. **Professional Services**. In order to implement Customer’s use of the Service, Company will provide to Customer the professional services described in the Customer’s Order Form and/or any associated Statement of Work (SOW). Each SOW will include, at a minimum: (a) a description of the Professional Services and training deliverables to be provided to Customer (“**Deliverable**”); (b) the scope of Professional Services; and (c) the applicable fees for such Professional Services. All SOWs shall be deemed part of and subject to this Agreement.

   i. *Scope Changes*. If Customer requests a change in any of the specifications, requirements, or scope (including drawings and designs) of the Professional Services described in any SOW, then Customer will propose the applicable changes by written notice. After receipt of the proposed change, each party’s project leads shall meet within a reasonable time, either in person or via telephone conference, to discuss and agree upon the proposed changes. Company will prepare a change order (“**Change Order**”) describing the proposed changes to the SOW and the applicable fees and expenses, if any. Change Orders are not binding unless and until they are executed by the Parties. Executed Change Orders shall then become a part of the SOW and subject to this Agreement.

   ii. *Training Deliverables*. If printed materials are required by Customer, then Customer is solely responsible for any printing, shipping, and copying charges. All electronic and hard copy versions of the training Deliverables are provided for Customer’s internal training purposes only. Except for Customer’s internal use, Customer is prohibited from: (i) modifying the training Deliverables (ii) utilizing the training deliverables to replicate or attempt to perform the training for third parties and (iii) reselling or sublicensing any training Deliverables. Subject to terms and conditions of this Agreement, and during the term hereof, Company hereby grants to Customer a limited, non-exclusive, non- transferable, terminable license to use the Deliverables solely for Customer’s internal operations in connection with its authorized use of the applicable Service.

   iii. *Subcontracting.* Company reserves the right to use third parties (who are under a covenant of confidentiality with Company), including, but not limited to, offshore subcontractors to assist with the Professional Services, including, without limitation, any data migration, configuration, and implementation processes.

   iv. *Professional Services Warranty*. Company warrants that: (i) Company and each of Company’s employees (consultants and subcontractors, if any), that provide and perform Professional Services has the necessary knowledge, skills, experience, qualifications, and resources to provide and perform the Professional Services in accordance with any applicable SOW; and (ii) the Professional Services will be performed for and delivered to Customer in a good, diligent, workmanlike manner in accordance with industry standards. Company’s ability to successfully perform hereunder is dependent upon Customer’s provision of timely information, access to resources, and participation.

   v. *Fees.* Professional Services/Implementation fees are earned upon performance and non-refundable.

3. **Customer Data and Security**

   a. **Customer Data**. Customer must provide data for use of the Services and Company. Customer remains solely responsible at all times for the content and accuracy of the Customer Data and for ensuring that the Customer Data complies with the terms of this Agreement and the DPA. Company has no obligation to monitor or pre-screen any Customer Data uploaded, generated, stored, or transmitted by Customer as part of, or in conjunction with, the Services.

   b. **Ownership of Customer Data**. As between Company and Customer, all Customer Data is owned exclusively by Customer, including Reports. Customer grants Company the right to use the Customer Data solely for purposes of performing under this Agreement. If the return of Customer Data is requested by Customer, export of such data will be in CSV format using the standard export functions provided by the Services.

   c. **Security**. Company will implement and deploy security features, procedures and technologies that will, in accordance with Applicable Law, and best industry practices, provide protection from unauthorized access to or use, disclosure, modification, transmission or destruction of Customer Data and other data hosted in connection with the Services and Applications. More information on particularities of data processing can be found within the Company's Data Processing Agreement (DPA) (incorporated by reference and/or attached as Exhibit B).

4. **Confidentiality and Property Rights**.

   a. **Confidentiality**. Each party agrees to use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (at all times exercising at least a commercially reasonable degree of care in the protection of such confidential information) not to use or disclose Confidential Information except to the extent necessary to perform its obligations or exercise rights under this Agreement or as directed by Customer. Either party may disclose Confidential Information on a need to know basis to its Affiliates, contractors and Companies who have executed binding written agreements requiring confidentiality and non-use obligations at least as restrictive as those in this Agreement. Either party may disclose Confidential Information to the extent that such disclosure is required by law or order of a court or other governmental authority.

   b. **Service and Documentation Intellectual Property Rights**. All rights, title, and interest in and to the Service (including without limitation all intellectual property rights therein and all modifications, Source Code, extensions, customizations, scripts, or other derivative works of the Service provided or developed by Company) are owned exclusively by Company or its licensors. Except as provided in this Agreement, the rights granted to Customer do not convey any rights in the Service, express or implied, or ownership in the Service or any intellectual property rights thereto. Any rights in the Service or Company's intellectual property not expressly granted herein by Company are reserved by Company. Company alone shall own all right, title, and interest, including all related intellectual property rights, in and to the Documentation, and any suggestions, ideas, requests, feedback, recommendations, or other information provided by Customer or any other party relating to the Services and Documentation

   c. **API (if applicable).** Company provides access to its application-programming interface ("**API**") as part of the Service and may charge as described on the Order Form or SOW. Subject to the other terms of this Agreement, Company grants Customer a non-exclusive, nontransferable, terminable license to interact only with the Service as allowed by the API.

   d. **Injunctive Relief**. The Receiving Party acknowledges that disclosure or use of Confidential Information in violation of this Agreement could cause irreparable harm to the Disclosing Party for which monetary damages may be difficult to ascertain or an inadequate remedy. The Receiving Party therefore agrees that the Disclosing Party will have the right, in addition to its other rights and remedies to seek injunctive relief for any violation of this Agreement, without posting a bond and without prejudice to any other rights and remedies that the Disclosing Party may have for breach of this Agreement.

   e. **Destruction or Return of Confidential Information**. Within forty-five (45) days of termination or expiration of the Agreement, or upon Disclosing Party's written request, Recipient will, at the Disclosing Party's direction, promptly dispose of or return the other party's Information. Notwithstanding the foregoing, Recipient will not be required to return to the Disclosing Party or destroy copies of Disclosing Party's Confidential Information that Recipient is obligated by applicable law or governmental regulations to retain. All copies retained under this Section will remain subject to all confidentiality obligations under this Section.

5. **Payment**. Customer must pay all fees as specified on the Order Form, but if not specified, then within 30-days of receipt of an invoice. Customer is responsible for the payment of all sales, use, VAT, and other similar taxes. Company's invoices shall be deemed correct and acceptable to Customer unless Customer advises Company of disputed items within ninety (90) days of receipt of such invoice. During any renewal term (i.e., only after the Initial Term), subscription fees may increase by no more than five percent (5%) per year (the "Renewal Percentage").

6. **Availability Warranty and Disclaimer**.

   a. **Limited Warranty**. Company warrants to Customer that the Services will substantially conform with generally accepted industry standards of care and competence for other providers of similar hosted solutions. Notwithstanding anything to the contrary herein, Company has no warranty obligations: (a) to the extent that Services were modified by Customer or any third party, unless the modification was approved in writing by Company; (b) for problems caused by any third-party software or Hardware, or (c) by other matters beyond Company's reasonable control including interruptions to the Service related to emergency maintenance.

   b. **Compliance with Laws.** Company represents and warrants that it will comply with all applicable federal, state, and local laws and regulations with respect to the Services**.**

   c. Software Warranty.

   Company represents and warrants that the software, if any, as delivered to Customer, does not contain any program code, virus, worm, trap door, back door, time or clock that would erase data or programming or otherwise cause the software to become inoperable, inaccessible, or incapable of being used in accordance with its user manuals, either automatically, upon the occurrence of licensor-selected conditions or manually on command.

   Company further represents and warrants that all third-party software, delivered to Customer or used by Company in the performance of the Agreement, is fully licensed by the appropriate licensor

   d. EXCEPT AS EXPRESSLY PROVIDED HEREIN OR IN A STATEMENT OF WORK, COMPANY DOES NOT WARRANT THAT ACCESS TO THE APPLICATIONS, SOFTWARE OR SERVICES WILL BE UNINTERRUPTED OR ERROR FREE, NOR DOES COMPANY MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. FURTHER, COMPANY MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO SERVICES PROVIDED BY THIRD PARTY TECHNOLOGY SERVICE PROVIDERS RELATING TO OR SUPPORTING HOSTING AND MAINTENANCE SERVICES. THE APPLICATIONS, SOFTWARE AND SERVICES ARE PROVIDED "AS IS," AND OTHER THAN THE SERVICE LEVEL WARRANTY, COMPANY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. **Indemnification**.

   a. **Company Intellectual Property Indemnity**. Company shall defend and indemnify Customer from any claims, suits, actions, or proceedings brought against Customer in a court of competent jurisdiction by a third party which allege that the Customer's use of the Services otherwise not in violation of any of the terms this Agreement causes an infringement of such third party's intellectual property rights and any judgment finally awarded in respect of such Claim, for which all avenues of appeal have been exhausted, or any final settlement of such Claim, to the extent that such Claim arises solely as a result of Customer's use of the Services in accordance with the provisions of the Agreement, and provided: (a) Customer notifies Company in writing within thirty (30) days of Customer first becoming aware of each such Claim; (b) Customer does not make any admission against Company's interests and Customer does not agree to any settlement of any Claim without the prior written consent of Company; (c) Customer, at the request of Company, provides all reasonable assistance to Company in connection with the defense, litigation, and/or settlement by Company of the Claim; and (d) Company has sole control over the selection and retainer of legal counsel.

b. Intellectual Property Warranty and Indemnification**.** Company represents and warrants that any materials or deliverables, including all Deliverable Materials, provided under this Agreement are either original, or not encumbered, and do not infringe upon the copyright, trademark, patent or other intellectual property rights of any third party, or are in the public domain. If Deliverable Materials provided hereunder become the subject of a claim, suit or allegation of copyright, trademark or patent infringement, Customer shall have the right, in its sole discretion, to require Company to produce, at Company's own expense, new non-infringing materials, deliverables or works as a means of remedying any claim of infringement in addition to any other remedy available to the Customer under law or equity. Company further agrees to indemnify, defend, and hold harmless the Customer, its officers, employees and agents from and against any and all claims, actions, costs, judgments or damages, of any type, alleging or threatening that any Deliverable Materials, supplies, equipment, services or works provided under this contract infringe the copyright, trademark, patent or other intellectual property or proprietary rights of any third party (Third-Party Claim of Infringement). If a Third-Party Claim of Infringement is threatened or made before Company receives payment under this Agreement, Customer shall be entitled, upon written notice to Company, to withhold some or all of such payment.

8. **Limitations of Liability**.

a. **Exclusion of Indirect Damages.** NEITHER PARTY SHALL BE LIABLE UNDER THIS AGREEMENT FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR LOST PROFITS), EVEN IF THE OTHER PARTY HAS BEEN INFORMED OF THIS POSSIBILITY.

b. **Total Limit on Liability.** EXCLUDING ANY CLAIMS DUE TO A PARTY'S GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT, AND CLAIMS FALLING UNDER SECTION SEVEN (7) , EITHER PARTY'S TOTAL LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT, TORT, OR OTHERWISE) SHALL NOT EXCEED THE AMOUNT OF FEES PAID OR PAYABLE BY CUSTOMER TO COMPANY UNDER THIS AGREEMENT IN THE TWELVE (12) MONTH PERIOD. HOWEVER, COMPANY'S MAXIMUM LIABILITY FOR ANY CLAIMS RESULTING FROM WRONGFUL DISCLOSURE OF STANDARD PERSONAL INFORMATION WILL NOT EXCEED THREE TIMES (3X) THE FEES PROPERLY DUE AND OWING UNDER THE AGREEMENT.

9. **Insurance.** Prior to the commencement of this Agreement and throughout the Term, Company will maintain insurance coverages with the limits described herein. Such insurance shall be with insurers rated A-VII or higher by A.M. Best and issued by an insurance company or companies authorized to do business in the United States (or any other country where the Services are used). Company shall, at its expense, during the entire Term of the Agreement and at all times while it has any obligations remaining under this Agreement, keep in full force and effect policies of insurance meeting or exceeding the specifications set forth below with respect to the performance of its obligations under this Agreement: (i) Commercial general liability with limits of not less than $1,000,000 per occurrence and $2,000,000 in the aggregate, such insurance shall include but not be limited to products/completed operations liability, blanket contractual liability, personal injury liability and broad form property damage. Such insurance shall be (1) primary for all purposes and (2) contain standard cross liability provisions, (ii) business automobile liability insurance with combined single limit for bodily injury and property damage of not less than $1,000,000 (iii) Worker's compensation insurance with statutory limits, and employer's liability insurance with limits not less than $1,000,000,000, (iv) Professional Liability/Errors and omissions liability insurance with limits not less than $1,000,000 per occurrence and $5,000,000 in the aggregate; covering liability and defense costs arising out of the acts, errors or omissions, of Company and its agents, contractors and employees, the failures and errors of any products provided by Company, (v) Cyber liability insurance (also known as "privacy and network security liability insurance") with limits not less than $1,000,000 per occurrence and $2,000,000 in the aggregate; covering claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering or the failure of Company to protect the security of any computer or other electronic network. The Cyber liability policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses. The Company and their insurance carriers agree to waive the right to subrogation under Workers Comp policy.Upon reasonable request, Company will provide Customer proof of all insurance in force pursuant to this Section. Any modifications decreasing policy limits or cancelations of the policies shall be provided to Customer at least thirty (30) days prior to taking effect.

The City of San Diego, it's respective elected officials, officers, employees, agents and representatives shall be additional insureds, on a primary and non-contributory bases, under the Commercial General Liability policy specified above per the additional insured general liability blanket endorsement.

10. **Suspension/Termination**.

a. **Suspension for Delinquent Account**. Company reserves the right to suspend Customer's and any Customer Affiliates' access to and/or use of the Service if any payment is due but unpaid, but only after Company has provided Customer one (1) delinquency notice following Customer's failure to pay and at least thirty (30) days have passed since the transmission of the first notice.

b. **Suspension for Ongoing Harm**. Company may with reasonably contemporaneous telephonic notice to Customer suspend access to the Service if Company reasonably concludes with evidence that Customer's account is being used to engage in denial-of-service attacks, spamming, or illegal activity, and/or use of Customer's account is causing immediate, material and ongoing harm to Company or others. In the event Company suspends access to the Service, Company will use commercially reasonable efforts to limit the suspension to the offending portion of the Service and work with Customer to resolve the issues causing the suspension of Service. Any suspension under this section shall not excuse Customer from Customer's obligation to make payments under this Agreement.

c. **Termination for Cause**. Either party may immediately terminate this Agreement and all Order Forms issued hereunder in the event the other party commits a material breach of any provision of this Agreement which is not cured within thirty (30) days of written notice from the non-breaching party. Such notice by the complaining party shall expressly state all of the reasons for the claimed breach in sufficient detail so as to provide the alleged breaching party a meaningful opportunity to cure such alleged breach. A Party may also terminate if the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within thirty (30) days.

d. **Termination Upon Annual Renewal**. Notwithstanding any language to the contrary in the Customer's Order Form, upon thirty (30) days' written notice prior to the expiration of each year of the Term, either Party may terminate this Agreement for convenience.

e. **Effect of Termination**. Upon termination or expiration of this Agreement, Customer shall have no rights to continue use of the Service. If this Agreement is terminated by Customer for any reason other than for cause or Upon Annual Renewal, then Company shall be entitled to all of the fees due under this Agreement. If this Agreement is terminated as a result of Company's breach of this Agreement, then Customer shall be entitled to a refund of the pro rata portion of any unused, prepaid Service fees paid by Customer to Company under this Agreement for the terminated portion of the Term.

11. **General Provisions**.

a. **Entire Agreement, and Amendment**. This Agreement, any applicable Order Form(s), SOW, SLA, and the DPA constitute the entire understanding between the Parties, and accordingly the Parties (i) expressly disclaim any reliance on any and all prior discussions, emails, or RFP's concerning the subject matter hereof (ii) acknowledge there are no verbal agreements, representations, or warranties between the Parties; and (iii) acknowledge that any terms and conditions included within a Purchase Order (PO) or Invoice provided by the Customer shall not apply and are deemed invalid. The Agreement shall not be modified, or amended, except in writing and signed by the Parties.

b. **Governing Law and Jurisdiction**. This Agreement is governed by the substantive and procedural laws of the State of California.

c. **Assignment**. Neither Party may assign or transfer any of the rights, duties or obligations herein without the prior written consent of the other Party. Any attempted assignment will be null and void, with no force or effect. Notwithstanding the foregoing, a Party shall have the right to assign this Agreement without the other Party's consent: (i) if to any Affiliate or (ii) if to any successor in interest by merger or by purchase of substantially all of its assets; provided such assignee executes a written assumption of this Agreement.

d. **Severability**. If any provisions herein are held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force without being impaired or invalidated in any way. The Parties agree to replace any invalid provision with a valid provision that most closely approximates the intent and economic effect of the invalid provision.

e. **Survival.** Sections concerning Confidentiality, Ownership of Customer Data, Intellectual Property Rights, Limitation of Liability, and Indemnification shall survive the termination or expiration of this Agreement.

f. **Notice**. Any notice required under this Agreement shall be provided to the other party in writing. If Customer wishes to provide a notice to Company, then notice should be sent to: 5300 Memorial Drive, Suite 300, Houston, Texas 77007, Attention: Legal Department or if by email, legalnotice@iOfficecorp.com. If Company wishes to provide a notice to Customer, other than operational notices provided by email, then notice should be sent to the address and/or email address provided below Customer's signature.

g. **Force Majeure**. Neither Party will be responsible nor liable for any delays or failures in performance from any cause beyond its control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, weather conditions, or internet service providers. The non-delayed Party may terminate this Agreement if such failure or delay continues for a period of 30 days or more and, if the non-delayed Party is Customer, receive a refund of any unused, pre-paid Service fees to the Company in advance for the affected Services.

h. **No third-Party beneficiaries**. All terms and conditions of this Agreement shall be binding upon and shall inure to the benefit of the Parties hereto and their successors and authorized assigns. Except as otherwise provided in this Agreement, nothing in this Agreement, express or implied, is intended or shall be construed to create any rights in, or confer any benefits upon, any person or entity other than the Parties to this Agreement.

i. **Independent Contractors.** Company's relationship with Customer pursuant to this Agreement will be that of an independent contractor. Neither party will have any authority to bind the other, to assume or create any obligation, to enter into any agreements, or to make any warranties or representations on behalf of the other. Each party is solely responsible for all of its employees and agents and its labor cost and expenses and for any and all claims, liabilities or damages or debts of any type whatsoever that may arise on account of each Party's activities or those of its employees or agents in the performance of this Agreement.

j. **Material changes**. Customer must immediately notify Company in writing of any change in their business operations, financial condition, licenses, or regulatory approvals if the change is likely to have a material adverse effect on Company's ability to perform its obligations under this Agreement.

SIGNATURE PAGE

Authorized representatives of CUSTOMER and COMPANY have read the foregoing and all documents incorporated therein and agree and accept such terms effective as of the latter signature date below.

CITY OF SAN DIEGO
A Municipal Corporation

By: ______________________________

Printed Name: Claudia C. Abarca

Address for Notice:1200 Third Avenue, Suite 200
San Diego, CA 92101

Email for Notice: lhoffmann@sandiego.gov

Title: Director, Purchasing & Contracting Department

Date Signed: Dec 22, 2022

Approved as to form this 23 day of December, 20 22

MARA W. ELLIOTT, City Attorney

By: Jane Boardman
Jane Boardman (Dec 23, 2022 09:06 PST)
Deputy City Attorney

ManagerPlus Solutions, LP

By: Dan Bisanz
Dan Bisanz (Dec 23, 2022 13:12 EST)

Printed Name: Dan Bisanz

Title: VP Finance

Date: Dec 23, 2022

Accounts Payable Contact

Name: Maria Cummins

Title: Account Clerk

Tel: (619) 235-5932

Email: MCummins@sandiego.gov

Is a PO required? Yes

EXHIBIT A

Order Form/SOW Details

Customer Name: City of San Diego
Order Number: Q-13227
Quote Expires: 12/28/2022
Quote Term (months): 12
Payment Frequency: Annual

Item	Qty	Description	Annual Amount
Lightning Experience - Named User	71.00	A license specific to an individual allowing access to the browsersoftware and mobile apps (iOS & Android)	USD 57,510.00 (taxable)

Recurring Annual Total: USD 57,510.00

Item	Qty	Description	One-Time Amount
Onboarding Standard Package	1.00	The Standard Package includes up to 30-days of on-boarding from the date of purchase. See attached SOW document for onboarding details. (Includes 2 hours online training)	USD 2,295.00
Online Training	4.00	Online training for Admins and Supervisors	USD 1,200.00
Professional Services	3.00	3 days of onsite training for Admins and Supervisors - See statement of work fordetails	USD 8,900.00

One Time Total: USD 12,395.00
Quote Total: USD 69,905.00

Sales Tax is Not Included

Order Form Provisions

Licensing & Term	
Subscription Effective Date:	December 28, 2022
Term of Subscription:	One (1) year beginning with Subscription Effective Date (the 'Initial Term')
Payment Terms	
Currency:	USD
Payment Frequency:	Annual
Invoice Date:	Beginning of each Term
Invoice Terms:	Customer shall be invoiced annually in advance for Services provided.
Payment Due Date:	Net 30
Permitted Renewal Increase	During any Renewal Term (after the Initial Term), subscription fees may increase by no more than 5% per year (the "Renewal Percentage")
Renewal & Price Changes	
Law & Jurisdiction	
Applicable Law	All agreements with Customer will be construed pursuant to the laws of the State of California.
Jurisdiction for Disputes	Any legal action or proceeding relating to the Agreement shall be instituted in a state or federal court in the jurisdiction of the first defendant in such action, and each party hereby consents to personal jurisdiction in such jurisdiction.
Dispute Resolution	Any dispute, controversy or claim arising out of or relating to the Agreement, shall, if the parties are unable to resolve such matter, be finally settled by binding arbitration between the parties pursuant to the commercial arbitration rules of the American Arbitration Association. The arbitration shall be conducted in the jurisdiction above before a single arbitrator. The arbitration award may be enforced by application to any court of competent jurisdiction.

Project Summary

Payment Terms

Project Name	City of San Diego Lightning Upgrade
Client Name	City of San Diego
Client’s Administrator	Clayton Walsten
Estimated Project Cost	$12,395

Statement of Work ("SOW")

Any requirements not included herein or items not contemplated, will be considered outside the scope of the SOW and will be handled through the Change Order process defined in the Professional Services Agreement and may result in additional costs.

Term
This SOW shall commence as of the date of December 28, 2022 ("Effective Date") and approved by the City Attorney in accordance with Charter section 40, and thereafter expire when the Customer's subscription and/or license to use the Services expires according to the term on the Customer's Order Form or if the Agreement is terminated for reasons herein.

Scope

The scope of this document is to provide explanation and to detail the in-scope tasks and associated costs related to the implementation of ManagerPlus Lightning. It will serve as the guiding document providing clarity to expectations, goals and intent to the project. The scope of this project includes the following primary objectives:

Module(s).

The scope of this project includes the following primary objectives:

- **Create a Lighting Cloud Database from a Customer Provided ManagerPlus [Standard, Pro, Desktop] Backup**
- **Dashboards and Monitoring – A series of dashboards are available in Lightning to manage and monitor performance of assets and system utilization. Corporate level dashboards as well as site and regional dashboards are provided. Configuration of existing dashboards and monitoring capability that can be completed within the 30-Day project period.**

Responsibilities

<u>ManagerPlus Responsibilities</u>
The functionality defined in this scope will be deployed over a 30-day period and this deployment will be managed by an assigned ManagerPlus implementation specialist. The assigned implementation specialist will schedule the initial kickoff meeting and weekly meetings as needed to support the deployment on the agreed schedule of the Lightning Modules, Dashboards and Reports defined below. The weekly meeting will include a status update by ManagerPlus on the deployment progress and a review of any open issues and related action items.
ManagerPlus will support the loading of data into the lightning application as stated in the Data Provisioning section of the SOW.

<u>Client Responsibilities</u>
The client is responsible for ensuring Subject Matter Experts are available for the Kickoff and jointly scheduled meeting to support process review, data provisioning, testing, training, and integration support if included in the SOW. Client is responsible for the collection, formatting and cleanliness of all data as detailed in the Data Provisioning sections. Client is responsible for providing training room, flip chart and markers, projector, or screen & HDMI connector for sharing, and for scheduling attendees for agreed upon onsite sessions. All attendees must have a computer with access to City network and a log-in to Lightning to attend training. The trainer will need connectivity Wi-Fi and access to log-in to the Lightning environment while onsite.

Joint Responsibilities
ManagerPlus and City of San Diego will have joint responsibility for the design and mapping of interfaces to external business systems. In general, ManagerPlus will be responsible for the integration mapping of the Lightning component to third party SW application or to a middleware application. City of San Diego will be responsible for the mapping of the third-party SW application to Lightning or to a middleware application. Both parties will consult on the interface strategy and build schedule.

Data Provisioning

City of San Diego will provide ManagerPlus with a .BAK file of both their On-Prem ManagerPlus database and Attachments related to the ManagerPlus database.

ManagerPlus will provide City of San Diego with instructions and a SharePoint file location to upload said .BAK files at the project Kickoff Meeting. City of San Diego will provide all data to be loaded into ManagerPlus Lightning by the following milestone in the 30-day implementation period:

- All required data provided to iOFFICE within 10 working days after the kickoff meeting
- After completion of admin sessions, the upload of a second more recent backup of City of San Diego’s On-Prem can be scheduled to be completed at schedule date, known as the go live date. This date represents the date that City of San Diego will stop using the On-Prem and exclusively move all operations to Lighting Cloud. If no second load of data is needed, then a go live date will be set to move customer to the adoption phase.

Data Delay Options: If the milestone for client to deliver data for ManagerPlus is not met, ManagerPlus and City of San Diego will meet to discuss the impact on the project and the options to move forward, which may include:

- ManagerPlus support as provided in the Purchase Order for the upgrade from Manager Plus Enterprise to support collection and formatting of data
- A new SOW for data collection with a fixed price estimate. This will require working with City of San Diego to determine issues impacting data collection and the estimate to complete.
- A hold on the project with firm dates for City of San Diego to complete data collection

Assumptions

Unique Identifiers

The identification of asset and maintenance records requires that all major assets and facilities adhere to a common naming convention.

Asset ID’s: The Asset ID is a unique name or identifying number given to a piece of equipment. The Asset ID must be 24 characters or less. It is important to note that M+ receives data from other systems such as GPS and Hours tracking systems. The common denominator between these multiple systems is the Asset ID so the Asset ID must match for all integrations.

All additional service hours will as provided in the Purchase Order for the upgrade from Manager Plus Enterprise or be billed at Implementation Services stated Hourly Rate and will use Standard terms unless otherwise negotiated. All additional services will be agreed upon with client prior to any work being performed.

Travel Expenses - Priced per Site Visit – Invoiced at cost as Required as provided in the Purchase Order for the upgrade from Manager Plus Enterprise.

Training

Administrator Training
Administrator Training will be scheduled with City of San Diego during the implementation period and must be completed within the implementation period. All admin training will be conducted remotely.

- All admin education is only consumable during the 30-day implementation period
- All admin education sessions are not to exceed 1 hour per session
    - Administration Training for 30-day implementation – 6 hours
- Data and/or administrator training requested beyond the implementation period will be subject to additional costs

Post-implementation Group End User Training

Group end user training is to train end users on the system. This training is interactive and prepares attendees to begin using ManagerPlus. Group end user training is conducted via webinar and will consist of pre-determined topics and an opportunity for questions and answers with a live trainer at the end of the session. Group training may have multiple customers on each session. A full list of training sessions available is located on the ManagerPlus Learning Center website.

Onsite Training

A 3-day onsite visit to be scheduled within 90 days of completion of implementation. After implementation, please compile a list of items that you would like to cover during this visit. There will be a 1-hour prep call at least 2 weeks in advance to confirm the dates, review the compiled list of topics, agenda, and attendees. Training may include end-user or administrative training on any module. Report building, data loading, and re-configuration is out of scope for this visit. Training hours are limited to a maximum of 8 hours per day.

Change Management Process

Any changes to the project scope listed in the SOW will be addressed and implemented by a scope amendment. Costs associated with any change will be reviewed with City of San Diego and included in the scope amendment.

Onsite Training Related Expenses

Client is responsible for a $2000 travel expense fee and $2000 per day of onsite training as provided in the Purchase Order for the upgrade from Manager Plus Enterprise.

Licensing

ManagerPlus, an iOFFICE Company, owns and retains all rights to software created and developed by ManagerPlus. The Client is not licensed to resell, transfer, or distribute any software or services created by ManagerPlus.

Miscellaneous

Confidentiality Notice:
The information contained in this document is confidential and proprietary to ManagerPlus. It is provided solely for the use of Client to detail the approach and work to be accomplished for Client’s implementation. This information may not be used for any other purpose and may not be further distributed. Review of this document shall constitute agreement to the restrictions stated above.

No Recording:
Customer shall not film or record ManagerPlus' delivery of the Professional Services, company resources, or company materials.

Cancellation/ Postponement:
ManagerPlus and Client shall use reasonable efforts to attend all scheduled requests. The repeated cancelation of meetings may result in delay and additional costs.

License Procurement:
Any rights for Client to use the Subscription Services are outside the scope of this SOW and must be separately procured by Client from ManagerPlus pursuant to an Order Form.

Disclaimer:
This SOW and the Professional Services Agreement terms shall constitute the entire understanding between Client and ManagerPlus and is intended as the final expression of the Parties' agreement regarding the Professional Services to be provided by ManagerPlus. The Parties expressly disclaim any reliance on any and all prior agreements, understandings, RFP's, verbal and/or written communications related to the Professional Services to be provided by ManagerPlus.

Acceptance and Authorization

The terms and conditions of the **Professional Services Agreement** apply in full to the services and products provided under this Statement of Work.

IN WITNESS WHEREOF, the parties hereto each acting with proper authority have executed this Statement of Work, under seal.

City of San Diego	ManagerPlus Solutions, LP
Claudia Abarca	Dan Bisanz
Full name	Full name
Director, Purchasing & Contracting	VP Finance
Title	Title
	Dan Bisanz Dan Bisanz (Dec 23, 2022 13:12 EST)
Signature	Signature
Dec 22, 2022	Dec 23, 2022
Date	Date

EXHIBIT B

DATA PROCESSING AGREEMENT (DPA)

Combined GDPR Personal Data and CCPA Personal Information Processing Agreement

This DPA is by and between iOFFICE, LP., with its wholly owned subsidiaries: Hippo Facility Management Technologies, Inc., Teem Technologies, LLC, and ManagerPlus Solutions, LP, ("**Processor**" and/or "**Data Importer**"), on the one hand, and CUSTOMER ("**Controller**" and/or "**Data Exporter**") on the other. Controller and Processor are sometimes referred to herein individually as a "Party" and collectively as the "Parties."

This Data Processing Agreement ("**DPA**") supplements the Agreement between Customer and Company that governs the Products and Services described in the Order Form giving the Customer access and use to the Products and Services which is incorporated by reference ("**Agreement**"). This DPA shall be effective as of the Effective Date Agreement and approved by the City Attorney in Accordance with Charter section 40.

DEFINITIONS

Unless otherwise defined herein or in the Agreement, capitalized terms and expressions used in this DPA shall have the following meaning:

"**Applicable Data Protection Laws**" means any and all laws and regulations applicable to the processing, privacy or security of Personal Data under the Agreement, including, but not limited to: the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and the laws implementing or supplementing the GDPR, the UK Data Protection Act 2018; and the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 et seq. ("“**CCPA**"), as each may be amended from time to time and – where applicable - the local data protection law of Data Controller, and any binding decisions of courts, tribunals or the relevant Regulator or, in each case, its successor data protection law.

"**Company**" means iOFFICE, LP as described above.

"Customer Data" means all electronic data or information submitted to and stored in the Service by Customer and its Users. Personal data may include (a) Personal Information as defined within the CCPA or GDPR; (b) identifies an individual, including by name, email address, telephone number; and (c) pertains to an individual's medical history, physical condition, or medical treatment.

"**Data Controller**" or "**Controller**" shall have the same meaning as in the Applicable Data Protection Laws and shall include without limitation: (i) the entity which alone or jointly with others, determines the purposes and the means of the processing of Customer Data (ii) the data exporter in the EU Standard Contractual Clauses; and (iii) entities defined as a "Business" under the CCPA;

'**Data Processor"** or "**Processor**" shall have the same meaning as in the Applicable Data Protection Laws and shall include without limitation: (i) the entity which processes Personal Data on behalf of the Data Controller; (ii) the data importer in the EU Standard Contractual Clauses; (iii) entities defined as a "Service Provider" under the CCPA or any entity permitted to use Personal Data pursuant to a permissible business purpose in accordance with restrictions prohibiting, among other things, the sale of any Personal Data in accordance with the CCPA. Exempt under the CCPA; and (iv) any other entity who has obtained or received Personal Data from a Data Controller and who may process such Personal Data as permitted by, or in accordance with, Applicable Data Protection Laws.

"**Data Subjects**" means a Consumer under the CCPA, a Data Subject under the GDPR, or other natural person granted similar rights under other Privacy and Security Laws.

"**Data Transfer**" means: (i) a transfer of Customer Data from the Customer to a Subprocessor; or (ii) an onward transfer of Customer Data from a Processor to a Subcontracted Processor, or between two establishments of a Subcontractors, in each case, where such transfer would be prohibited by Data Privacy and Security Laws;

"Privacy and Security Laws" means any and all international, local, country-specific, and U.S. State and Federal laws, regulations, directives, standards, policies, and procedures, as amended, applicable to Company pertaining to the security, confidentiality, or privacy of Customer Data.

"**Process**" means to perform, whether or not by automatic means, any operation or set of operations on Customer Data, including without limitation to (a) collect, receive, store, host, organize, combine, log, catalog, cross-reference, maintain, copy, or translate; or (c) erase, delete, or destroy.

"Security" means Company's technological, physical, administrative, and procedural safeguards, including, without limitation, policies, procedures, guidelines, practices standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is, in whole or part: (a) to protect the confidentiality, integrity or availability of Customer Data; and (b) to prevent the unauthorized use of or unauthorized access to Customer Data.

"Services" means the service(s) that Company provides to Customer directly or through any subcontractor under the terms of the Agreement or any applicable Statement of Work ("SOW").

"Standard Contractual Clauses" (incorporated herein by reference) means the legal mechanism for the transfer of personal data as set out in the GDPR, incorporated by reference. The Standard Contractual Clauses will apply to Customer Data that is transferred from the EEA to outside the EEA, either directly or via onward transfer, to any country or recipient: not recognized by the European Commission as providing an adequate level of protection for Customer Data (as described in the GDPR).

"**Subprocessor**" means any person appointed by or on behalf of Processor to process Customer Data on behalf of the Customer in connection with the Agreement.

"**Users**" means individuals who are authorized by Customer or its Affiliate to use the Service pursuant to the Agreement or as otherwise defined, restricted, or limited in an Order Form or amendment, for whom subscriptions to a Service have been procured. Users include but are not limited to Customer's and Customer's Affiliates' employees, consultants, contractors, and agents.

1. DATA PROCESSING

1.1 **Controller Instructions.** Processor shall only Process Customer Data to the extent necessary to provide the Service(s) to Customer and/or as set forth in the Agreement, an applicable SOW and for no other purpose. Customer acknowledges and agrees that Customer is the Controller of such Customer Data and Customer remains responsible for the obligations of a Controller, including but not limited to, the responsibility for complying with any laws and regulations providing for notice, choice, and/or consent prior to transferring the Personal Data to Processor for Processing. Customer shall disclose Personal Data to Processor only as necessary for Processor to provide the Services. Without limiting Processor's obligations under this agreement, Processor has no obligation to monitor or pre-screen the content or accuracy of Customer Data uploaded, generated, stored, or transmitted by Controller as part of, or in conjunction with the Services. The Parties expressly agree and stipulate that the DPA, including applicable service level agreements or equivalent documents, shall constitute Controller's written instructions to Processor. Any additional processing instructions must be mutually agreed to in writing by the Parties. Processor shall immediately inform Controller if, in Processor's opinion, an instruction infringes Applicable Law.

1.2 **Authority to Transfer to Processor.** Controller represents and warrants that Controller has the authority and right, including consent where required, to lawfully transfer to Processor all Personal Data and any other data or information related to Controller's access or use of the services provided under the DPA.

1.3 **Compliance with Applicable Law.** Company shall not retain, use or disclose Customer Data for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by the Privacy and Security Laws. Company acknowledges and agrees that it shall not retain, use or disclose Customer Data for a commercial purpose other than providing the Services. In performing their respective obligations under the terms of this DPA, each party warrants that it shall comply with (and shall ensure that its staff and/or subcontractors comply with: (i) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective which apply to the services being provided under the Agreement and relate to the privacy, confidentiality, and/or security of Personal Data, including, but not limited to, GDPR and CCPA, (collectively, "Data Protection Laws")and (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security which apply to the services being provided under the Agreement.

1.4 **Processor Personnel.** Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Subprocessor who may have access to the Customer Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Data, as strictly necessary for the purposes of the Agreement, and to comply with Privacy and Security Laws in the context of that individual's duties to the Subprocessor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

1.5 **Sale of Personal Data.** Personal Data provided to or collected by Processor on behalf of Controller in connection with Services does not constitute a "sale" of personal data under Data Protection Laws. Processor will not rent or sell Personal data to any party for monetary or other valuable consideration. Processor agrees to refrain from taking any action that would cause any transfer of Personal data to Processor to qualify as a sale of Personal Data under the Data Protection Laws.

1.6 **Wellness Feature (if applicable).** Controller consents to the processing of special category data, more specifically, data concerning a User's health. "Data concerning health" means personal data related to the physical health of a natural person which reveals information about his or her health status.

2. THIRD PARTIES; SUB-PROCESSORS

2.1 Processor shall only provide Customer Data or access to the Customer Data to those subcontractors or other third parties to the extent necessary for Processor to perform Services for Customer. Once the subcontractor or other third party no longer needs access to the Customer Data in order for Processor to perform Services for Customer, Processor shall immediately terminate such access, or, if applicable, shall immediately request that Customer terminate such access.

2.2 Processor shall provide to Customer a complete list of subcontractors who will Process Customer Data in furtherance of Processor's provision of Services to Customer at the outset of the Agreement, and shall update the list as necessary, provided however that Processor shall not engage a subcontractor to Process Customer Data except as explicitly set forth herein.

2.3 Processor shall not provide any subcontractor or third party (other than Processor's regulator) with access to Customer Data or access to Processor's systems or network that would allow access to Customer Data, unless (i) Processor has received prior written or general consent from Customer, which shall not unreasonably be withheld; or (ii) such access is specifically allowed under this DPA, the Agreement, or an applicable SOW. Processor shall notify Customer immediately upon receipt of any request from a regulator to access Customer Data, including any request to access locations where such information is stored.

2.4 **Engagement of sub-processors.** Except as otherwise agreed in writing in this DPA, the Processor shall not engage another processor without prior specific or general authorization of the Controller. Where the Controller has given a general written authorization to engage other processors, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors and give Controller the opportunity to object to such changes. Notwithstanding the foregoing, Controller expressly acknowledges and agrees that Processor may retain any entity which is controlled by, controls or is in common control with Processor ("**Affiliates**"), where such Affiliates are subject to Processor's security policies and the data protection requirements of this Agreement, in connection with the provision of the services provided under the Agreement.

2.5 **Obligations of sub-processors.** Any sub-processors will be permitted to process Personal Data only as necessary to deliver the services being provided under the Agreement and for which Processor has retained them, and such sub-processors are prohibited from processing Personal Data for any other purpose. Such sub-processors will provide services pursuant to a written agreement containing the same data protection obligations as set forth herein. Processor shall be liable to Controller for the acts and omissions of its sub-processors to the same extent Controller would be liable if performing the services of each sub-processor directly under the terms of this DPA.

2.6 **List of Sub-processors.** Upon Controller's request, Processor shall make available to Controller a current list of Sub-processors for the respective services with the identities of those Sub-processors ("**Sub-processor List**").

3. CONFIDENTIALITY

3.1 **Confidentiality.** Processor will treat Personal Data provided by Controller as confidential. Processor will ensure that its personnel engaged in the processing of Personal Data provided by Controller are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and are subject to obligations of confidentiality and that such obligations survive the termination of that persons' engagement with Processor.

4. SECURITY PROCEDURES

4.1 **Security Measures (Exhibit A).** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the processing of Personal Data implement appropriate technical and organizational measures to protect the security, confidentiality, integrity, and availability of Personal Data provided by Controller, as set forth in further detail in Appendix 2.

4.2 **Data Breach Notification.** Processor shall promptly notify Controller (and in any event within twenty-four (24) hours) after becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data of Controller or its User(s) ("**Data Breach**") after having become aware of such Data Breach. Notification(s) of Data Breaches, if any, will be delivered to Controller's designated contact by means as agreed to by the Parties. Notification(s) shall, to the extent known by the Processor: (i) describe the nature of the Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) communicate the name and contact details of the Processor's data protection officer or other contact point where more information can be obtained; (iii) describe the likely consequences of the Data Breach; and (iv) describe the measures taken or proposed to be taken by the processor to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Processor shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Data Breach.

5. ASSISTANCE TO CONTROLLER

5.1 **Data Subject Rights.** Where possible, and taking into account the nature of the processing, Processor will provide reasonable assistance to Controller for the fulfillment of Controller's obligation to respond to requests for exercising data subjects' rights as set forth in GDPR, Articles 12-23 or other applicable Data Protection Laws requiring Controller to provide similar rights to data subjects. Processor shall not respond to such requests from data subjects except on instructions from Controller, unless required by applicable laws to which Processor is subject, in which case Processor shall inform Controller of that legal requirement before responding to the request.

5.2 **Security and Data Protection Impact Assessments.** Processor will provide reasonable assistance to Controller for the fulfillment of Controller's obligations pursuant to GDPR under Articles 32 to 36, or where required pursuant to other applicable Data Protection Laws to which Controller is subject, to: (i) ensure the security of the processing; (ii) notify the relevant supervisory authority, and any data subject(s), where relevant, of any breaches relating to Personal Data; (iii) carry out any data protection impact assessments of the impact of the processing on the protection of Personal Data; and (iv) consult the relevant supervisory authority prior to any processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Controller to mitigate the risk; in each case as appropriate and feasible with respect to the nature of processing and information available to Processor.

5.3 **Audits and Inspections.** Processor shall make available to Controller information necessary to demonstrate compliance with the obligations set forth in GDPR, Article 28 or the CCPA. Processor shall allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller. Before the commencement of any such on-site audit, Processor and Controller shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Controller shall be responsible. The Parties shall work in good faith to schedule the audit at a time that is mutually beneficial, and so as to avoid unreasonable disruption to Processor's business operations. Unless otherwise agreed to in writing by the Parties, each party shall bear its own costs associated with the performance of audits of Processor conducted pursuant to this provision. Controller shall promptly notify Processor with information regarding any non-compliance discovered during the course of an audit relevant to the services being provided under the Agreement or this DPA.

6. DATA TRANSFERS

6.1 **Transfer to United States (Non-US Users).** Controller expressly acknowledges that some or all of the Services may be provided and/or hosted from within the United States. Controller expressly consents to the transfer of Controller's Personal Data to the United States (or shall procure such consent from its customer(s) to the extent that such Personal Data is being processed on behalf of the Controller's customer(s)) for the purposes of Processor providing the services and performing its obligations under the Agreement. Such transfers will be conducted pursuant to this DPA, including the Standard Contractual Clauses. In the event that a valid data transfer mechanism upon which Controller and/or Processor relies for transferring Personal Data for the provision of Services is amended, replaced or repealed under Data Protection Laws, the parties shall work together in good faith to negotiate a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws.

7. PERSONAL DATA DELETION

8.1 Deletion or Return of Personal Data. Upon expiration or termination of the Agreement, all licenses granted herein shall terminate, and each Party shall return to the other, or purge from its electronic or other storage facilities or records, all property (including any Confidential Information) of the other Party in its possession or control. In addition, within forty-five (45) days any termination, or upon Customer's request, and at no additional cost to Customer, Company shall export all Customer Data from the Services in an electronic format reasonably requested by Customer. Upon written request, Company will provide an affidavit affirming destruction.

9. MISCELLANEOUS

9.1 Duration. Unless otherwise agreed to in writing by the Parties, this DPA shall remain in effect until the later of the expiration of the Agreement or the deletion or return of Personal Data in accordance with Section 8.1.

9.2 Insurance Coverage. In addition to any insurance requirements specified in the Agreement or any Exhibit thereto, Processor shall also maintain Privacy and Network Security (otherwise known as Cyber Liability) coverage which includes providing protection against liability for (a) system attacks, (b) denial or loss of service attacks, (c) spread of malicious software code, (d) unauthorized access and use of computer systems, (e) crisis management and customer notification expenses, (f) privacy regulatory defense and penalties and (g) liability arising from the loss or disclosure of data that would encompass Customer Data; with an annual aggregate of no less than five million dollars $5,000,000. Processor shall maintain such insurance coverage during the Term of this DPA and for at least six months (6) months after expiration or termination of this Agreement.

9.3 Failure to Perform. In the event that changes in law or regulation render performance of this DPA impossible or commercially unreasonable, the Parties may renegotiate this DPA in good faith. If renegotiation would not cure the impossibility, or the Parties cannot reach an agreement, the Parties may terminate the Agreement for Services in accordance with the Agreement's termination provisions.

9.4 Updates. Company may update the terms of this DPA from time to time; Company will provide prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services. Notices will be sufficient if provided (i) to a user designated as an administrator of your applicable account; (ii) as a note on the screen presented immediately after completion of the log in authentication credentials at the log in screen; or (iii) by email to the registered email address provided for the administrator(s) for Customer's account.

Authorized representatives of Customer and Company have read the foregoing and all documents incorporated therein and agree and accept such terms effective as of the latter signature date below.

CITY OF SAN DIEGO

By:__________________________

Name: Claudia Abarca

Title: Director, Purchasing & Contracting

Date: Dec 22, 2022

ManagerPlus Solutions, LP

By: Dan Bisanz
Dan Bisanz (Dec 23, 2022 13:12 EST)

Name: Dan Bisanz

Title: VP Finance

Date: Dec 23, 2022

Email for Customer Data Notifications: CWalsten@sandiego.gov (Clayton “Wally” Walsten)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter uses the Data Importer’s services for the full scope of activities outlined in the Agreement, which are incorporated herein by reference, as if fully set forth at length below. Without limitation, these services include automated functions to support asset, office, and facilities management and support conference room, desk, and visitor management.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Data Importer processes user information for the data exporter to provide office and facilities management services, which information can include first, middle, and last name, aliases, employee ID or username, job title, mobile, work, and personal phone numbers, email addresses, mail stop, building, floor, and room location for employees, as well as other, related information, including other forms of personal data, germane to the work environment and office and facilities management.

Processing may also include user information for the data exporter to provide provide conference room and visitor management services, which information can include calender unique identifier, color, name, and access control status (read only, or read-write) of calendars. Event unique identifier, title (or subject), description (or comments), location, recurring (true or false), dates and times of the event, visibility (private or no), and if the meeting is all day (true or false). Name and email address of all attendees.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Data subjects in scope include application users, employees, owners, directors, facility visitors, customers, and vendors.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Data Importer processes user information for the data exporter to provide office and facilities management services, which information can include first, middle, and last name, aliases, employee ID or username, job title, mobile, work, and personal phone numbers, email addresses, mail stop, building, floor, and room location for employees, as well as other, related information, including other forms of personal data, germane to the work environment and office and facilities management.

Processing may also include user information for the data exporter to provide provide conference room and visitor management services, which information can include calender unique identifier, color, name, and access control status (read only, or read-write) of calendars. Event unique identifier, title (or subject), description (or comments), location, recurring (true or false), dates and times of the event, visibility (private or no), and if the meeting is all day (true or false).Name and email address of all attendees.

Special categories of data (Wellness Feature)
The personal data transferred concern the following special categories of data (please specify): Heath related data.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

If AUP is utilized, a directory watcher will consume the file upon receiving. On consumption the file will be parsed into a temp table and compared to our current user set. Data importer will calculate the Delta data and update accordingly. The AUP file is then archived in a secure location where it is kept for 60 days or until space is needed, upon which it time the data is purged. Data is stored in the application is retained for reporting purposes until the end of contract.

Other processing includes, storage, the use of databases, analysis, queries, and the use of automated code to provide the services detailed in the Agreement or which are necessary or helpful to provide the services described in the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer also has mechanisms or processes in place to provide for:

- the pseudonymisation or encryption of data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The technical and organisational measures (TOMs) in place, based on context, are included in Exhibit A – Information Security Requirements.

Exhibit A – Information Security Requirements

Throughout the Term, Company will adopt and maintain appropriate (including organizational and technical) security measures in dealing with the Confidential Information and Customer Data in order to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In determining the technical and organizational security measures required under the Agreement, Company will take account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Company shall maintain processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Company agrees to the following with respect to all Confidential Information and Customer Data.

1. **Safeguards – Program.** Company will implement appropriate safeguards to protect Confidential Information and Personal Data that are consistent with accepted industry practices (such as ISO 27001 / 27002, ITIL, COBIT or other industry standards of information security), and will ensure that all such safeguards comply with Data Protection Law and the Agreement, including the Data Processing Agreement (DPA) where applicable.

2. **Safeguards – Specific.** At a minimum, Company's information safeguards will include: (a) secure facilities, data centers, paper files, servers, back-up systems and computing equipment including, but not limited to, all mobile devices and other equipment with information storage capability; (b) network, device application, database and platform security; (c) secure transmission, storage and disposal; (d) authentication and access controls within applications, operating systems and equipment; (e) logging material access and exfiltration, and retention of such access control logs for a period of at least one (1) year; (f) encryption of Personal Data at rest including when stored on any electronic notebook, portable hard drive, or removable electronic media with information storage capability; (g) encryption of Personal Data when transmitted over public or wireless networks; (h) separation of Personal Data from information of Company's other customers; (i) personnel security and integrity including, but not limited to, background checks consistent with applicable law; (j) annual external and internal penetration testing and vulnerability scans and promptly implementing, at Company's sole cost and expense, a corrective action plan (including timeline) to correct material issues that are identified through testing; and (k) limiting access of Personal Data, and providing privacy and information security training, to Company's Authorized Personnel. "Authorized Personnel" means Company's personnel who have a need to know or otherwise access Personal Data to enable Company to perform its obligations under the Agreement, and who are bound in writing by obligations of confidentiality sufficient to protect Personal Data in accordance with the terms of the Agreement, including the DPA where applicable.

3. **Malware.** Company will not introduce to Reseller's Affiliate's, or Customer's systems, networks, or devices or use any software or code that contains any virus, malware, ransomware, keylogger, logic bomb, Trojan horse, worm, or other software routines designed to: (a) permit unauthorized access to Reseller's, Affiliate's or Customer's systems, networks, or devices; (b) disable, erase, or otherwise harm software, hardware, or data owned or controlled by Reseller, Affiliate, Customer; or (c) record or monitor any persons access to Reseller's, Affiliate's, or Customer's systems, networks, or devices.

4. **Banned Hardware or Equipment.** Company shall not utilize hardware or equipment that does not comply with Section 889(a)(1)(B) of the National Defense Authorization Act for Fiscal Year 2019. Company will provide representation of compliance with this provision to Reseller upon request. If Company believes it can no longer comply with this provision, Company will notify Reseller immediately by sending an email to privacy@iofficecorp.com.

5. **Disaster Recovery and Business Continuity.** Company will maintain and implement as necessary a business continuity and disaster recovery plan ("BCDR Plan") which shall include at a minimum: (a) documentation of applicable business processes, procedures and responsibilities; (b) back-up methodology; (c) identification of

disaster recovery scenarios and service level agreements for service recovery; (d) responsibilities of Sub-Processors in the event of a disaster; (e) a communications strategy; and (f) procedures for reverting to normal service. The DRBC Plan shall be reviewed annually. Company shall ensure it is able to implement the DRBC Plan at any time in accordance with its terms. Company shall test the DRBC Plan on a regular basis (and, in any event, not less than annually). Upon request, Company shall send to Reseller a written report summarizing the results of the most recent test and shall promptly implement any actions or remedial measures which Reseller and Company mutually agree to be necessary as a result of those tests.

6. **Cooperation with Audits.** Company will during the Term and upon Reseller's reasonable request: (a) promptly provide to Reseller such records as are required to verify the Company's performance and processes in relation to compliance with the requirements of this Agreement including compliance with applicable laws ("**Compliance Requirements**"); (b) allow for and contribute to audits, including inspections, conducted by Reseller (or a third party auditor designated by Reseller), and performed based on a mutually agreed upon scope, timing, and duration; and (c) where a regulatory body requires an audit, allow Reseller and/or (as mutually agreed by Company and Reseller) a designated third party and/or a regulator to audit the Company's premises, sites, and records as are required to verify the Company's adherence to any Compliance Requirements.

   Any audit shall be carried out on reasonable prior written notice of no less than thirty (30) days and shall not be carried out more than once a year, except in the event of a Security Incident. Access to Company premises for the purposes of such an audit or inspection is subject to: (a) the production of reasonable evidence of identity and authority by the auditors; (b) normal business hours; (c) audit personnel have committed themselves to confidentiality by executing written confidentiality obligations; and (d) access only to information that is strictly relevant to the Services provided to or on behalf of Reseller or Reseller's Affiliates. Each party is responsible for its own costs arising from contributing to audits. If material gaps are identified during the course of an audit, Company shall use commercially reasonable efforts to remediate material gaps within a timeframe reasonably agreed upon by the Parties.

   If Reseller is at any time not reasonably satisfied with the remediation efforts, the Parties shall negotiate in good faith to reach agreement on new technical and organizational security measures. The Parties acknowledge that if they are unable to reach agreement thereafter, Reseller shall have the right, notwithstanding anything to the contrary in the Agreement, to terminate this Agreement.

1-City_of_San_Diego_Agreement_2022-12_15

Final Audit Report 2022-12-23

Created:	2022-12-22
By:	Lisa Hoffmann (lhoffmann@sandiego.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA5Zp9A_fOAyLtCi5k6z0ewyiDWtPiMBCc

"1-City_of_San_Diego_Agreement_2022-12_15" History

Document created by Lisa Hoffmann (lhoffmann@sandiego.gov)
2022-12-22 - 4:10:39 PM GMT- IP address: 156.29.5.177

Document emailed to Claudia Abarca (CAbarca@sandiego.gov) for signature
2022-12-22 - 4:24:37 PM GMT

Email viewed by Claudia Abarca (CAbarca@sandiego.gov)
2022-12-23 - 1:31:05 AM GMT- IP address: 156.29.5.177

Document e-signed by Claudia Abarca (CAbarca@sandiego.gov)
Signature Date: 2022-12-23 - 1:31:45 AM GMT - Time Source: server- IP address: 156.29.5.177

Document emailed to jboardman@sandiego.gov for signature
2022-12-23 - 1:31:46 AM GMT

Email viewed by jboardman@sandiego.gov
2022-12-23 - 3:27:18 AM GMT- IP address: 104.28.111.133

Signer jboardman@sandiego.gov entered name at signing as Jane Boardman
2022-12-23 - 5:06:31 PM GMT- IP address: 156.29.5.190

Document e-signed by Jane Boardman (jboardman@sandiego.gov)
Signature Date: 2022-12-23 - 5:06:33 PM GMT - Time Source: server- IP address: 156.29.5.190

Document emailed to dan.bisanz@eptura.com for signature
2022-12-23 - 5:06:34 PM GMT

Email viewed by dan.bisanz@eptura.com
2022-12-23 - 6:11:49 PM GMT- IP address: 104.47.55.254

Signer dan.bisanz@eptura.com entered name at signing as Dan Bisanz
2022-12-23 - 6:12:24 PM GMT- IP address: 76.145.234.80

Document e-signed by Dan Bisanz (dan.bisanz@eptura.com)

Signature Date: 2022-12-23 - 6:12:26 PM GMT - Time Source: server- IP address: 76.145.234.80

Agreement completed.

2022-12-23 - 6:12:26 PM GMT