Master Agreement

This Master Agreement (this "**Master Agreement**"), effective on the date of the last Party signature below and approved by the City Attorney ("**Effective Date**"), is between Zasio Enterprises, Inc., a California corporation with its principal offices at 401 W. Front St., Suite 305, Boise, Idaho 83702 ("**Zasio**"), and the City of San Diego, a California municipal corporation (the "**Customer**") (individually a "**Party**" and collectively, the "**Parties**").

This Master Agreement establishes the terms for Zasio's provision of those Products and Services (defined in Attachment B) and Zasio Services (defined in Attachment C) described in the Attachments to this Master Agreement (collectively the "**Zasio Offering(s)**"). Capitalized terms not defined in this Master Agreement are defined in their applicable Attachment.

NOW, THEREFORE, for good and valuable consideration, intending to be legally bound and pursuant to the terms and conditions of this Master Agreement, the Parties hereby agree as follows:

1. **Attachments**. The following are attached and form part of this Master Agreement:

Attachment A: Customer Required Terms

Attachment B: Master Software Licensing Agreement (Superseding)

- **Exhibit 1**: Pricing Table
- **Exhibit 2**: Software Support Terms and Conditions

Attachment C: Master Software as a Service and Records and Information Management (RIM) Professional Services Agreement

- **Exhibit 1**: Pricing Table
- **Exhibit 2**: Support Services Terms
- **Exhibit 3**: Service Level Guarantee
- **Exhibit 4**: Technical and Organizational Measures
- **Exhibit 5**: Zasio Records and Information Management (RIM) Professional Services Supplemental Terms
  - **Annex A to Exhibit 5**: Statement of Work
- **Exhibit 6**: City of San Diego Technical and Security Administrative Regulations

Order of Precedence. Attachment A shall take precedence over any terms in this Master Agreement and Attachments B and C, including their exhibits. Upon any conflict between Attachment A and this Master Agreement or Attachments B or C, including their exhibits, Attachment A will prevail.

2. **General Definitions**

"**Affiliate**" means any legal entity which directly or indirectly controls, is controlled by, or is under common control with, a Party. An entity controls another entity if it holds more than 50 percent of the other entity's shares or voting rights. All rights and benefits granted to Customer under this Master Agreement will extend to, and Zasio Offerings may be used and accessed by, Customer's Affiliates, provided that the use is in accordance with this Master Agreement. When this Master Agreement extends to a Customer Affiliate, the term Customer means that Affiliate. Customer shall remain responsible for all obligations under, and its Affiliate's compliance with, this Master Agreement.

"**Confidential Information**" means all information which the disclosing Party protects against unrestricted disclosure to others that the disclosing Party (or its representatives) designates as confidential, internal, or proprietary at the time of disclosure, or which should reasonably be understood as confidential at the time of disclosure given the nature and the circumstances surrounding its disclosure. Confidential Information includes Customer Data, a disclosing Party's trade secrets and proprietary information, the terms of this Master Agreement, the Software, Zasio Materials, pricing information for Zasio Offerings, and each Party's technology and related information, product designs, and business processes.

Confidential Information does not include information that (i) is known publicly at the time of disclosure by the disclosing Party or becomes publicly known after disclosure through no fault of the receiving Party; (ii) at the time of disclosure, is known to the receiving Party without confidentiality restrictions; (iii) is independently developed by the receiving Party without reference to the disclosing Party's Confidential Information; (iv) the receiving Party has lawfully acquired free of restrictions from a third party with the right to furnish the information; or (v) the disclosing Party agrees in writing is free of confidentiality restrictions.

"**Customer Data**" in respect of Products and Services means any data or information submitted by on behalf of Customer to Zasio to facilitate Zasio's provision of Products and Services. "**Customer Data**" in respect of Zasio Services means any data or information that (i) is submitted by or on behalf of Customer to Zasio (a) by uploading or storing it in the Hosted Services, or (b) to facilitate Zasio's provision of Zasio Services; or (ii) Customer derives from its use of the Hosted Services. In either case, Customer Data does not include Zasio Confidential Information, Zasio Materials, usage Data, or any Feedback.

"**Feedback**" refers to any idea for improving or otherwise modifying any Zasio Offering, Zasio's technology, or Zasio's business practices.

"**Hardware**" means any scanner or other physical equipment identified in an Order Form for Customer's use with Hosted Services. Hardware is sold by Zasio as a courtesy and "as is." Hardware may come with a manufacturer's warranty and Customer may purchase an extended manufacturer's warranty, which will be identified in the corresponding Order Form.

"**Order Form**" means the Pricing Table attached as **Exhibit 1** to Attachments B and C as well as any subsequently executed ordering agreements (including any statement of work) for Customer's purchase of additional Software and Support and Professional Services under Attachment B, or Zasio Services under Attachment C, that reference this Master Agreement. Upon execution by the Parties, an Order Form will become part of this Master Agreement. An Order Form may be terminated independent of this Master Agreement, pursuant to this Master Agreement.

"**Personal Data**" means all Customer Data relating to an identified or identifiable natural person.

"**Taxes**" means all transactional taxes, levies, fees, surcharges, and similar charges (and any related interest and penalties), such as federal, state, or local sales tax, value added tax, and goods and services taxes. Taxes do not include taxes based on Zasio's income, employees, property, or gross receipts.

"**Zasio Materials**" means anything created, provided, or made available by Zasio to perform this Master Agreement, including any reports, writings, works of art, ideas, source codes, citation texts and details, database scripts, trace documents, processes, inventions, designs, trademarks, trade names, or trade dress. Zasio Materials also means any process, method, design, or improvement (i) to the Software or the software forming part of the Hosted Services, or (ii) arising from Zasio's performing Support or Professional Services. Zasio Materials remain such whether or not protectable by patent, trademark, copyright, or trade secret. Zasio Materials do not include Customer Data, or any reports or deliverables provided or made available to Customer through Customer's use of Software.

3. Confidential Information

3.1 Confidential Information Use and Disclosure. The receiving Party shall not: (a) use the disclosing Party's Confidential Information except where required to exercise the receiving Party's rights or perform its obligations under this Master Agreement; or (b) disclose the disclosing Party's Confidential Information to any third party, except to the receiving Party's Personnel (defined in Attachment C), service providers, agents, or representatives who (i) are subject to confidentiality obligations at least as strict as this Master Agreement's, and (ii) have a need to know to carry out this Master Agreement.

3.2 Degree of Care. To protect disclosing Party Confidential Information, the receiving Party shall use at least the same degree of care that it uses to protect its own, similar Confidential Information; however, this must not be less than a reasonable degree of care.

3.3 Compelled Disclosure. The receiving Party may disclose disclosing Party Confidential Information to the extent required by law or order of a court or other government authority; however (and at the disclosing Party's cost), the receiving Party shall promptly, and prior to any disclosure, notify the disclosing Party of any request or demand for the disclosing Party's Confidential Information (unless prohibited by law), and provide reasonable assistance to contest the disclosure. The receiving Party shall use reasonable efforts to disclose only those portions of Confidential Information legally requested and required to be disclosed.

3.4 Confidential Information Destruction and Return. At the disclosing Party's request, the receiving Party shall promptly destroy or return the disclosing Party's Confidential Information (including copies and reproductions). This obligation does not apply: (a) as long as legal proceedings related to the Confidential Information prohibit its return or destruction; (b) to Confidential Information held in backup systems scheduled for deletion under standard backup policies; or (c) to Confidential Information the receiving Party may legally retain.

3.5 Disclosure Notice. Upon the unauthorized access, disclosure, or loss of, or inability to account for, any disclosing Party Confidential Information, the receiving Party shall promptly: (a) notify the disclosing party; (b) take reasonable steps to minimize the violation and resulting losses; and (c) cooperate with the disclosing Party to minimize the violation and any associated losses.

3.6 California Public Records Act. Nothing in this Master Agreement, including its Exhibits, shall prohibit Customer from disclosing information that qualifies as a 'public record' (as that term is defined in the California Public Records Act, codified in California Government Code section 7920.000 *et. seq.*) and which is not otherwise exempt from release under the provisions of the California Public Records Act.

4. Terms.

4.1 Limited Use of Personal Data. For purposes of the California Consumer Privacy Act ("CCPA"), Zasio is a service provider and Customer is a government entity and Zasio shall comply with all obligations applicable to a service provider, including those related to Personal Data privacy and security. Zasio shall not sell or share Personal Data (as those terms are defined under the CCPA, regardless of the CCPA's application). Zasio also shall not retain, use, or disclose Personal Data outside of the direct business relationship between Zasio and Customer or for a commercial purpose (as that term is defined in the CCPA). Zasio's access to any Personal Data is not part of the consideration exchanged in respect of this Master Agreement.

4.2 Legal Rights to Personal Data. If anyone contacts Zasio to exercise a legal right with respect to Personal Data, Zasio shall promptly forward the request to Customer and shall not respond except to inform the individual of this. Zasio shall promptly and reasonably assist Customer to fulfil any individual request to exercise their rights under applicable data privacy law, including a request to access, delete, opt-out, or receive information about the processing of Personal Data pertaining to them. Notwithstanding the foregoing, Zasio acknowledges and agrees that Customer is not a business under the CCPA and is not subject to the obligations of a business under the CCPA. Customer has sole responsibility to notify Zasio if Customer believes that Personal Data provided to Zasio under this Master Agreement becomes subject to any privacy or security requirements from jurisdictions that are not incorporated into this Master Agreement. If this happens, the Parties shall work in good faith to include the additional requirements in an amendment.

4.3 Term and Termination of Master Agreement.

4.3.1 Subject to Section 7 (License Term and Attachment B Term) of Attachment B, and Section 7 (Subscription and Attachment C Term) of Attachment C, the term of this Master Agreement is for an initial term of one year with additional four one-year option terms at the sole discretion of Customer. Customer may, in its sole discretion, unilaterally exercise an option to extend the Master Agreement with written notice to Zasio no less than 30 days before the expiration of the term then in effect. The Master Agreement term cannot exceed five years unless approved by the City Council of Customer by ordinance.

4.3.2 Customer may terminate this Master Agreement, including its Attachments, without cause by providing Zasio with a written termination notice delivered pursuant to this Master Agreement's notice requirements.

4.3.3 Upon terminating an Attachment pursuant to the express terms of that Attachment, the terminating Party may elect to also terminate this Master Agreement, including any remaining Attachments, by providing written notice of the same within 60 days.

4.3.4 Either Party may immediately terminate this Master Agreement upon written notice if the other Party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit to creditors.

4.3.5 If either Party terminates this Master Agreement, or any Attachment, for cause or convenience, Zasio shall provide a prorated refund for any unused portion of a terminated Support Services term.

4.4 **Surviving Terms**. Any obligation under this Master Agreement, including those expressly identified in Attachments A, B, and C, that cannot be performed prior to termination, or that cannot be ascertained until after termination, or which by its nature or intent are to survive, will survive this Master Agreement's termination,

5. Liability Limitations.

5.1 No Party's liability arising out of or relating to this Master Agreement shall exceed the amount of fees paid or payable by Customer under the Order Form initially giving rise to the claim. This limitation shall apply regardless of the theory of liability or recovery, such as in tort, or contract, or otherwise.

5.2 No Party shall be liable for any special, indirect, incidental, consequential, exemplary, or punitive damages, including, for example, loss of good will, cost of procurement of substitute goods or services, loss of technology rights or services, loss of opportunity or business profits, loss of data, or business interruption.

5.3 As the sole exceptions to Section 5.1 and 5.2 above, neither Party excludes or limits liability for:

a. death or bodily injury arising from either party's negligent or willful misconduct;

b. Customer's unauthorized use of any Zasio Offering or Customer's failure to pay any fees due under this Master Agreement;

c. Damages resulting from the other Party's breach of Master Agreement Section 3 (Confidential Information);

d. Damages resulting from gross negligence, willful or fraudulent misconduct;

e. Misappropriation of the other Party's intellectual property (proprietary rights including patents, trademarks, copyrights, and trade secrets);

f. Its express defense and indemnification obligations under Attachments B or C; or

g. Any liability exclusion or limitation that cannot be limited pursuant to applicable law.

6. General Terms

6.1 Assignment. Neither Party may assign this Master Agreement or any portion of it without the other Party's express written consent, which will be in that other Party's sole discretion. However, any merger, consolidation, or reorganization involving Customer (regardless of whether Customer is a surviving or disappearing entity) will not require Zasio's written consent; provided that no transfer will relieve Customer of any of its obligations under this Master Agreement and Customer provides Zasio timely written notice of the transfer.

6.2 Waiver and Amendment. A Party's waiver of any term of this Master Agreement must be in writing and signed by both Parties. Otherwise, a Party's failure or delay to exercise any right is not a waiver of that right or any other. The Parties may amend this Master Agreement only by written amendment signed by both Parties. A written amendment also must specifically refer to this Master Agreement and state the Parties' intent to amend the Master Agreement.

6.3 Nature of Services. Zasio is not a law firm and does not provide legal advice or services. All decisions related to record retention, recordkeeping, and record destruction should be reviewed and approved by Customer's legal counsel.

6.4 Export Control Obligations. United States export laws and regulations, and any other relevant export laws and regulations, may apply to any Zasio Offering provided under this Master Agreement. Any applicable export control laws and regulations govern Customer's use of all Zasio Offerings provided under this Master Agreement. Customer shall comply with all applicable export laws and regulations. Customer shall not export data, information, software, or materials resulting from any Zasio Offerings (or any direct product of these) in violation of these laws.

6.5 Force Majeure Event. Neither Party shall be liable to the other for any failure or delay in performance, or breach, including for any resulting damages by the other Party, due to circumstance beyond the Party's reasonable control, including strike, riot, act of terrorism, natural catastrophe, failure of utilities, acts of God, or viral pandemic (a "**Force Majeure Event**"); provided, however, the non-performing Party promptly notifies the other Party and takes reasonable steps to minimize the disruption caused by the Force Majeure Event.

6.6 Feedback. Customer may elect to provide Zasio with Feedback, in which case Zasio has sole discretion to retain, use, and commercially exploit the Feedback without any obligation to Customer.

6.7 Independent Contractors. The Parties are independent contractors. Neither Party is the agent or partner, or has any power to act on behalf, of the other Party.

6.8 Severability. If any part of this Master Agreement is held invalid or unenforceable, the remaining parts will not be affected.

6.9 Equitable Relief. A Party's material breach of Section 3 (Confidential Information) of the Master Agreement, Section 2 (Software License and Restrictions) of Attachment B, or Section 3 of Attachment C (Customer Obligations and Restrictions) would cause the non-breaching Party irreparable harm for which money damages alone would be an inadequate remedy; accordingly, the non-breaching Party may pursue equitable relief in addition to any other remedies under this Master Agreement or at law, and without having to post a bond or prove actual damages.

6.10 Peaceful Resolution. Prior to taking legal action, the Parties shall attempt to resolve any dispute in connection with this Master Agreement amicably by negotiation, which may include mediation. However, either Party may seek provisional legal remedies if, in that Party's judgment, doing so is necessary to avoid irreparable harm.

6.11 Costs and Attorney's Fees. Reserved.

6.12 Governing Law and Jurisdiction. California law will govern all Zasio Offerings, and any other dispute under or arising out of this Master Agreement, excluding application of its choice of law provisions. A Party may bring an adversarial proceeding to resolve a dispute only in the state or federal courts in San Diego County, California, and the Parties agree that either of these courts would be a convenient forum. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

6.13 Notices. Unless otherwise expressly permitted in this Master Agreement, all notices required under this Master Agreement must be in writing and considered received (i) if mailed, the shorter period of either the notice's receipt or 5 days after mailing by registered mail; (ii) upon personal delivery; or (iii) if sent by email to the recipient Party's email contact (provided by the recipient Party), 24 hours after the email is sent or the first business day after it is sent, whichever is later. Notice to Customer will be as follows unless Customer has provided written notice to Zasio of a change:

City Clerk of San Diego, Diana Fuentes, 200 C ST, 2nd FLR, San Diego, CA 92101 (dfuentes@sandiego.gov)

6.14 Counterparts. This Master Agreement may be executed in one or more counterparts, each constituting an original. All counterparts must be construed together.

6.15 No Third-Party Beneficiaries. This Master Agreement is for the sole benefit of the Parties and nothing in it, express or implied, will confer upon any third-party any legal or equitable right, benefit, or remedy.

6.16 Taxes. All fees are exclusive of Taxes. All Taxes must be identified separately from the fees stated in the corresponding Order Form or invoice, as appropriate. Customer is responsible for payment of all Taxes applicable to Zasio Offerings. The Parties shall cooperate to legally minimize any applicable Taxes and obtain any exemption from, or reduced rate of, tax legally available. Customer is responsible for providing Zasio with any valid tax exemption certificate authorized by the appropriate taxing authority.

6.17 General Representations. Each Party represents that it has legal authority to enter into and perform its obligations under this Master Agreement. Zasio shall comply with all laws applicable to its performance under this Master Agreement.

6.18 Entire Agreement. This Master Agreement, including all its Attachments (including Attachment A) and other appendices; any executed Order Forms, SOWs, or change orders; and any accepted Renewal Documents, is the Parties' entire agreement, and supersedes any prior agreements concerning this subject matter. The Parties agree that any provisions in any Customer purchase, sales, confirmation, or acceptance order or document that are inconsistent with or in addition to any provision of this Master Agreement or Attachment A, shall be null and void, except with respect to any recital of the subject Zasio Offerings, such as quantities, price, descriptions, and delivery or subscription dates.

[*Signatures on the following page*]

The Parties have caused this Master Agreement to be executed by their duly authorized representatives to be effective as of the Effective Date.

ZASIO ENTERPRISES, INC.:	By: The City of San Diego
By: Cindy Zasio	Name- Diana Fuentes
Name: Cindy Zasio	Title: City Clerk
Title: VP of Operations	Address: 202 C St. SD, CA 92101
Date: January 26, 2024	Date: February 1, 2024

Approved as to form this 6th day of February, 2024

MARA W. ELLIOTT, City Attorney

By: Hilda R. Mendoza

Print name: Hilda R. Mendoza

Title: Deputy City Attorney

ATTACHMENT A to Master Agreement

This Attachment A to the Master Agreement ("Attachment A") is made part of and amends the Master Agreement by and between Zasio (referred to herein as "**Company**," "**Zasio**," "**Vendor**," or "**Contractor**") and Customer. Unless otherwise defined herein, capitalized terms shall have the definition set forth in the Master Agreement.

A. **Travel Expenses.** Notwithstanding anything herein, Customer will reimburse Zasio for expenses for any necessary pre-approved travel to San Diego for actual travel cost (coach air fare or car mileage) on the basis of fairness, reasonableness, and expenses considered customary as travel expenses by Customer. Customary travel related expenses include airfare, mileage, airport shuttles, car rental, hotel, and meals. Contractor shall base lodging and per-diem expenses on the most recent General Services Administration (GSA) standards for reimbursement for lodging and per-diem rates for San Diego, California. GSA standards may be located at this website: http://www.gsa.gov/portal/category/21287."

B. **Compensation.** Notwithstanding anything herein, Customer shall pay Zasio for performance of all services rendered and products provided under this Master Agreement in an amount not to exceed $1,500,000.

C. **Annual Appropriation of Funds.** Zasio acknowledges that the Master Agreement term may extend over multiple fiscal years of Customer, and that work and compensation under this Master Agreement is contingent on the City Council appropriating funding for and authorizing such work and compensation for those fiscal years. This Master Agreement, or any Attachment, may be terminated at the end of the fiscal year for which sufficient funding is not appropriated and authorized. Customer is not obligated to pay Zasio for any amounts not duly appropriated and authorized by City Council.

D. **Data upon Termination.** Subject to Section 4.9 of Attachment C (Return of Hosted Customer Data), upon expiration or termination of the Master Agreement or any Attachment, Zasio will immediately provide to the designated administrator for Customer electronic copies of any data collected and recorded in the format originally provided by Customer.

E. Section 8 of Attachment B and Section 10 of Attachment C, Limited Representations, Warranties, and Remedies, are hereby modified to add the following as new subsections "8.7" and "10.8" respectively:

"**8.7 and 10.8 Software and Intellectual Property Warranty.** Zasio represents and warrants that the software, if any, as delivered to Customer, does not contain any program code, virus, work, 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. Zasio further represents and warrants that all third party software, delivered to Customer or used by Zasio in the performance of this Attachment, is fully licensed by the appropriate licensor.

Zasio further represents and warrants that any materials or deliverables, including all deliverable materials, provided under this Attachment 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 Zasio to produce, at Zasio'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. Zasio further agrees to indemnify, defend, and hold harmless 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 Attachment 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 Zasio receives payment under this Attachment, Customer shall be entitled, upon written notice to Zasio, to withhold some or all of such payment."

F. Section 9 of Attachment B and Section 11 of Attachment C, Defense and Indemnification, are hereby modified to add the following as new subsections "9.5" and "11.5" respectively:

"**9.5 and 11.5 Customer Requirement.** Notwithstanding anything to the contrary in this Attachment, Zasio agrees and acknowledges that any agreement to settlements above certain dollar limits may require the approval of Customer's City Council pursuant to the provisions of Council Policy 000-09."

G. **Insurance**. Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by Contractor, his agents, representatives, employees or subcontractors.

Contractor shall provide, at a minimum, the following:

Commercial General Liability. Insurance Services Office Form CG 00 01 covering CGL on an "occurrence" basis, including products and completed operations, property damage, bodily injury, and personal and advertising injury with limits no less than $1,000,000 per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location (ISO CG 25 03 or 25 04) or the general aggregate limit shall be twice the required occurrence limit.

Commercial Automobile Liability. Insurance Services Office Form Number CA 0001 covering Code 1 (any auto) or, if Contractor has no owned autos, Code 8 (hired) and 9 (non-owned), with limit no less than $1,000,000 per accident for bodily injury and property damage.

Workers' Compensation. Insurance as required by the state of Contractor's operations, with Statutory Limits, and Employer's Liability Insurance with limit of no less than $1,000,000 per accident for bodily injury or disease.

Technology Professional Liability Errors and Omissions Insurance appropriate to the Consultant's profession and work hereunder, with limits not less than $3,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties.

Cyber Liability Insurance, with limits not less than $3,000,000 per occurrence or claim, $3,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

If Contractor maintains broader coverage and/or higher limits than the minimums shown above, City requires and shall be entitled to the broader coverage and/or the higher limits maintained by Contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to City.

Other Insurance Provisions. The insurance policies are to contain, or be endorsed to contain, the following provisions:

Additional Insured Status. The City, its officers, officials, employees, and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of Contractor including materials, parts, or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to Contractor's insurance (at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10, CG 20 26, CG 20 33, or CG 20 38; and CG 20 37 if a later edition is used).

Primary Coverage. For any claims related to this contract,
Contractor's insurance coverage shall be primary coverage at least as broad as ISO CG 20 01 04 13 as respects the City, its officers, officials, employees, and volunteers. Any insurance or self- insurance maintained by City, its officers, officials, employees, or volunteers shall be excess of Contractor's insurance and shall not contribute with it.

Notice of Cancellation. Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to City.

Waiver of Subrogation. Contractor hereby grants to City a waiver of any right to subrogation which the Workers' Compensation insurer of said Contractor may
acquire against City by virtue of the payment of any loss under such insurance. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the City has received a waiver of subrogation endorsement from the insurer.

Claims Made Policies (applicable only to professional liability). The Retroactive Date must be shown, and must be before the date of the contract or the beginning of contract work. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work. If coverage is canceled or non- renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, Contractor must purchase "extended reporting" coverage for a minimum of five (5) years after completion of work.

Self-Insured Retentions. Self-insured retentions must be declared to and approved by City. City may require Contractor to purchase coverage with a lower retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. The policy language shall provide, or be endorsed to provide, that the self- insured retention may be satisfied by either the named insured or City.

Acceptability of Insurers. Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A-VI, unless otherwise acceptable to City.

City will accept insurance provided by non-admitted, "surplus lines" carriers only if the carrier is authorized to do business in the State of California and is included on the List of Approved Surplus Lines Insurers (LASLI list). All policies of insurance carried by non-admitted carriers are subject to all of the requirements for policies of insurance provided by admitted carriers described herein.

Verification of Coverage. Contractor shall furnish City with original certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause. All certificates and endorsements are to be received and approved by City before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive Contractor's obligation to provide them. City reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.

Special Risks or Circumstances. City reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

Additional Insurance. Contractor may obtain additional insurance not required by this Contract.

Excess Insurance. All policies providing excess coverage to City shall follow the form of the primary policy or policies including but not limited to all endorsements.

Subcontractors. Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Contractor shall ensure that City is an additional insured on insurance required from subcontractors. For CGL coverage, subcontractors shall provide coverage with a format at least as broad as the CG 20 38 04 13 endorsement.

H. Section 6 of the Master Agreement, General Terms, is hereby modified to add the following sentence at the end of subsection 6.18, Entire Agreement:

"Notwithstanding the foregoing, the Parties agree and acknowledge that the Master Agreement is modified by Attachment A and to the extent there is a conflict between Attachment A and any portion of the Master Agreement, including any attachments and their exhibits, Order Forms, Statements of Work, or Renewal Documents, the language in Attachment A will control."

I. A new paragraph is added to the Master Agreement which will read as follows::
"Endorsement. Notwithstanding anything herein, Zasio shall comply with Council Policy 000-41 which requires that other than listing the City of San Diego as a client and other limited endorsements, any advertisements, social media, promotions or other marketing referring to the City as a user of a product or service will require prior written approval of the Mayor or designee. Use of the City Seal or City logos is prohibited."

J. A new paragraph is added to the Master Agreement which will read as follows:

"Contractor Standards. Zasio shall comply with the Contractor Standards provisions codified in San Diego Municipal Code section 22.3004(d). Zasio understands and agrees that violation of the Contractor Standards may be considered a material breach of the Master Agreement and may result in termination of the Master Agreement, including its attachments, debarment, and other sanctions."

K. A new paragraph is added to the Master Agreement which will read as follows:

"**Compliance with the Customer's Equal Employment Opportunity Outreach Program.** Zasio shall comply with the requirements of Customer's Equal Employment Opportunity Outreach Program as described in San Diego Municipal Code sections 22.2701 through 22.2708. Zasio shall not discriminate against any employee or applicant for employment on any basis prohibited by law. Zasio shall provide equal opportunity in all employment practices. Zasio shall ensure that its subcontractors comply with the Customer's Equal Employment Opportunity Outreach Program requirements. Nothing in this Section shall be interpreted to hold Zasio liable for any discriminatory practice of its subcontractors."

L. A new paragraph is added to the Master Agreement which will read as follows:

"**Americans with Disabilities Act.** Zasio shall comply with Customer's Council Policy 100-04, which provides that all City of San Diego vendors, including but not limited to construction vendors, consultants, grantees, and providers of goods and services, agree to comply with all applicable titles of the Americans with Disabilities Act."

M. A new paragraph is added to the Master Agreement which will read as follows:

"**Equal Benefits Ordinance Certification.** Unless an exception applies, Zasio shall comply with the Equal Benefits Ordinance codified in San Diego Municipal Code sections 22.4301 through 22.4308. Failure to maintain equal benefits is a material breach of the Agreement."

N. A new paragraph is added to the Master Agreement which will read as follows:

"**Business Tax Certificate.** Under this Master Agreement, Zasio is a provider of on-premises software licensing with associated software Support Services, Hosted Services with associated Support and Professional Services, and Records and Information Management Professional Services (collectively, Zasio Offerings), all provided remotely. Zasio's principal offices are located in Boise, Idaho. Zasio does not currently conduct business operations in the State of California. Should Zasio begin any operations in the City of San Diego, Zasio shall obtain a Business Tax Certificate (BTC) and to provide a copy of its BTC to the City."

O. A new paragraph is added to the Master Agreement which will read as follows:

"**Records Retention and Examination.** Zasio shall retain, protect, and maintain in an accessible location all records and documents, including paper, electronic, and computer records, relating to the Agreement for five (5) years after receipt of final payment by Customer under the Agreement.

Unless available electronically, Zasio shall make all such records and documents available for inspection, copying, or other reproduction, and auditing by authorized representatives of Customer, including the Purchasing Agent or designee. Zasio shall make available all requested data and records at reasonable locations within the City or County of San Diego at any time during normal business hours, and as often as Customer deems necessary. If records are not made available within the City or County of San Diego, Company shall pay Customer's travel costs to the location where the records are maintained and shall pay for all related travel expenses. Failure to make requested records available for inspection, copying, or other reproduction, or auditing by the date requested may result in termination of the Agreement. Zasio must include this provision in all subcontracts made in connection with this Agreement."

P. In the event of any conflict, inconsistency, or incongruity between the provisions of this Attachment A and any of the provisions of the Master Agreement, including any attachments, Order Forms, or Renewal Documents, the provisions of this Attachment A shall in all respects govern and control.

R. This Attachment A may be executed by one or more of the parties in any number of separate counterparts, each of which counterparts shall be an original, but all of which when together shall be deemed to constitute one and the same instrument. Any signature requirements of this Attachment A are satisfied by the Parties' signatures on the Master Agreement.

S. This Attachment A shall be construed in accordance with the laws of the State of California.

T. This Attachment A will be effective when signed by both parties and approved by the City Attorney, which signatures and approvals shall be evidenced by the Parties' full execution of the Master Agreement.

U. The terms of this Attachment A may not be terminated, amended, supplemented, or modified orally, but only by an instrument duly authorized by each of the parties.

Attachment B: Master Software License Agreement (Superseding)

This Master Software License Agreement ("**Attachment B**" or "**Attachment**"), effective on the date of the last Party signature on the Master Agreement and approved by the City Attorney ("**Effective Date**"), is between Zasio, and the City of San Diego, a California municipal corporation ("**Customer**") (individually, a "**Party**" and collectively, the "**Parties**").

The Master Agreement, and in particular this Attachment B, also supersedes the Parties existing software licensing agreement[s] with respect to Products and Services identified in the Recitals and Pricing Table (Exhibit 1 to Attachment B) below.

Recitals

Zasio is the developer and owner of certain records management, records retention, and related add-on software.

Customer previously purchased from Zasio licenses to the following on-premises software and related add-ons via separate licensing agreement[s]: Versatile Enterprise ("VE"), Versatile Enterprise Corporate Wide Access ("VE CWA"), Versatile Enterprise Records Management System ("ERMS"), and Versatile Records on-the-Go ("Mobile App") (the "Legacy Software").

Customer also desires to purchase licenses and related Support and Professional Services to the following Software: Versatile 2023, On-Premises, with Retention Schedule Management, U.S. Subscription (5-User Pack); Versatile Corporate-Wide Access for Versatile 2023 with Retention Schedule Management (Unlimited Users) (collectively, "New Software"). The Parties desire to have Customer's Legacy Software licenses, including any related Support and Professional Services, along with the New Software licenses, governed under a single licensing agreement and rescind all prior agreements.

Agreement

NOW THEREFORE, by entering into this Attachment B, the Parties agree that any prior software licensing agreements governing the above Products and Services, be governed by the Master Agreement (including Attachments A and B). This Attachment B shall also establish the terms for Customer's license to both the Legacy Software and New Software), along with Zasio's provision of any related Professional and Support Services, purchased pursuant to this Attachment B.

1. DEFINITIONS.

These capitalized terms are defined for this Attachment B as follows:

"**Add-on**" means any ancillary Software features and functionality licensed to Customer that support one or more corresponding Modules (such as the Versatile Notification System or Versatile Import Utility Add-ons).

"**Documentation**" when used in this Attachment B means Zasio's user and technical documents that Zasio makes available to Customer under this Attachment B that describe the Software's installation, functionality, components, features, configuration, use, support, maintenance, or requirements.

"**Internal Business Use**" when used in this Attachment B means the Customer's use for its own internal business operations on the Customer's systems, networks, and devices with Customer Data. This does not include Customer's use to provide services to or process data for, any third party, or use in a manner that is competitive to Zasio.

"**Module**" means a major set of related Software features and functionality being licensed to Customer, such as retention schedule management or physical records management.

"**Personnel**" means a Party's employees, contractors, or agents.

"**Pricing Table**" when used in this Attachment B means the document forming part of this Attachment B as **Exhibit 1**. The Pricing Table establishes the details and pricing information for the Software license, as well as any Professional Services and Support Services, that Customer has obtained under this Attachment B.

"**Products and Services**" means the Software, Support Services, and any Professional Services identified in an Order Form that Zasio provides to Customer under this Attachment B.

"**Professional Services**" when used in this Attachment B means optional implementation, on-site or remote training, configuration, integrations, data migration, and similar services related to the Software that are provided by Zasio. Any Professional Services that Customer purchases will be reflected in the applicable Order Form. Unless expressly stated otherwise in the applicable Order Form, Professional Services may be invoiced at their then current rate if not requested within 1 year of the applicable Order Form's effective date.

"**Purchased Plan**" means the category of access for each Module (such as the number of authorized users or jurisdictional scope of citations accessible) identified in an Order Form.

"**Software**" means Zasio's programs and applications, along with any add-on solutions, identified in an Order Form, licensed to Customer under this Attachment B. Software comes in executable form, and includes all related materials and Documentation, as well as all Updates, extensions, and derivatives, provided by Zasio.

"**Support Services**" when used in this Attachment B means Zasio's standard services the Customer has purchased from Zasio on an annual subscription basis to maintain and support the Software. Support Services are governed by this Attachment B and are described in more detail in Zasio's Support Terms and Conditions, which forms part of this Attachment B as **Exhibit 2**.

"**Updates**" when used in this Attachment B means modifications, additions, or adjustments to the Software, which Zasio has developed to: (i) correct bugs, deficiencies, or errors; (ii) conform to regulatory or industry requirements, or; (iii) incorporate improvements in operability. An Update does not include a separate product, provided under different terms, consisting of substantially different architectural features and functionality (even if such a product shares some common functionality with its predecessor).

2. SOFTWARE LICENSE AND RESTRICTIONS.

2.1 License. Zasio hereby grants Customer a perpetual (unless expressly stated otherwise in an Order Form), non-exclusive, non-transferable, non-sublicensable, non-assignable license to use the Software for Customer's Internal Business Use, subject to Customer's compliance with the restrictions in Section 2.3 below and Zasio's Termination for Cause rights in Section 7.3.

2.2 Software Installation. Customer may place a production copy of the Software on one server or workstation for each license Customer has purchased, as reflected in the Pricing Table. Customer must purchase a license for each server or workstation where the Software is installed. Regardless of the number of licenses, Customer may install three non-production copies of the Software for development, testing, and backup, which Customer may store off-site. If Customer transfers the Software's production copy from the designated installation site to another, Customer shall provide Zasio with a written statement detailing the transfer and certifying that the original Software and all copies have been removed from Customer's originally designated server or workstation, or both.

2.3 License Restrictions. Without Zasio's express written authorization, Customer shall not:

a. use, possess, or reproduce any Software in source code form;

b. distribute Software to, or allow any Software use by, a non-Personnel third party (including by renting, selling, leasing, or otherwise transferring);

c. decompile, disassemble, reverse-engineer, or otherwise attempt to discover any source code or underlying algorithms in the Software;

d. modify the Software or create derivative works from the Software; or

e. use the Software in a way that is competitive to any Zasio Product or Service.

However, Customer may reproduce or create derivative works of Documentation as reasonably necessary to support Customer's Internal Business Use of the Software.

2.4 Customer Personnel Use. Customer may permit its Personnel to use the Software under this Attachment B for Customer's Internal Business Use

3. Reserved.

4. DATA PRIVACY AND SECURITY.

4.1 Zasio's Security Program. In connection with Zasio's provision of Products and Services under this Attachment B, Zasio will maintain appropriate administrative, physical, and technical safeguards designed to protect Customer Data security and confidentiality, including measures designed to prevent the unauthorized access, use, modification, or disclosure of Customer Data. Customer Data will only be stored on systems and servers located in the United States. Zasio shall not retain, use, or disclose Customer Data for any purpose other than to provide Products and Services under this Attachment B.

4.2 Use of Third-Party Sub-processors. In connection with Zasio's provision of Products and Services under this Attachment B, Zasio may engage sub-processors to process Customer Data for purposes of performing this Attachment B; however, Zasio will not engage any sub-processor without including contractual terms with the sub-processor that are at least as protective as the terms of the Master Agreement and its attachments.

4.3 Customer Personal Data. The only kind of Personal Data that Zasio requires to provide Products and Services under this Attachment B is Personal Data (i) of Customer Personnel commonly known as business contact information (such as name, job title, employer, business email address, business telephone number, and the like); and (ii) consisting of limited bank and payment card details related to payment under this Attachment B. Customer shall use commercially reasonable efforts to minimize any transfer of Personal Data to Zasio to that appropriate to the Products and Services Customer purchases under this Attachment B.

4.4 Reserved.

4.5 Customer Control and Consent. In connection with Zasio's provision of Products and Services, Customer acknowledges that Zasio does not have access to Customer IT systems and servers, including all on-premises Software databases. Customer is solely responsible for the content and accuracy of all data that is uploaded or stored in the Software and all Customer Data disclosed to Zasio. Should Zasio process any Personal Data requiring an individual's consent, Customer shall obtain the individual's informed consent and provide this to Zasio upon request.

4.6 Legal Rights to Personal Data. Reserved.

5. INTELLECTUAL PROPERTY RIGHTS.

5.1 Proprietary Rights. The Software is licensed, and not sold, to Customer. Zasio retains all interests in the Software, including any related patent, trade secret, copyright, trademark, or other intellectual property rights, along with all Zasio Materials disclosed to Customer under this Attachment B.

5.2 Proprietary Notices. Customer will not remove, alter, or obscure any Zasio copyright, trademark, trade name, or other proprietary rights notices from any Products and Services, including in any copy.

5.3 Protection Against Unauthorized Use. Customer shall promptly notify Zasio of any unauthorized use, reproduction, or distribution of, or any unauthorized access to, the Software.

5.4 Customer Data. Between the Parties, Customer remains the exclusive owner of all rights in Customer Data. Customer grants Zasio a non-exclusive right to process and use Customer Data to provide Products and Services in accordance with this Attachment B.

6. FEES.

6.1 License and Service Fees. The fees for Software, Support Services, and any Professional Services purchased under this Attachment B are established in the corresponding Zasio Form(s). Should Customer request additional Professional Services, Zasio will provide these at its then standard rates unless the Parties reach another agreement in writing. Zasio shall invoice Customer for all reimbursable out-of-pocket expenses, including travel, lodging, and meals, in accordance with Customer's reasonable travel and expense policy, and with no additional markup.

6.2 Payment Terms. Zasio will submit to Customer invoices for all fees under this Attachment B. Customer shall pay all undisputed fee portions within 30 days of receipt. All payments must be in U.S. Dollars.

6.2.1 Software and Support Services. Upon delivery, Zasio shall invoice Customer for the Software and Support Services in the Pricing Table.

6.2.2 Renewal of Support Services. Renewal of the subscription term will be as set forth in section 7, below. Zasio will not increase annual Support Services fees by more than 4 percent per annum for any subsequent Support Services term and will provide written notice of any fee increase at least 45 days before beginning the new Support Services term.

6.2.3 Professional Services and Expenses. Zasio will invoice Customer for Professional Services and any applicable out-of-pocket expenses during the calendar month following their being incurred.

6.3 Reserved.

7. TERM AND TERMINATION.

7.1 License Term and Attachment B Term. Subject to the exceptions in Sections 2.3 and 7.3.2 of this Attachment B, the Software license under this Attachment B is perpetual. This Attachment B's term for any combination of Support Services or Professional Services is for an initial term of one year with additional four one-year option terms at the sole discretion of Customer. Customer may, in its sole discretion, unilaterally exercise an option to extend Attachment B with written notice to Zasio no less than 30 days before the expiration of the then current term in effect. The Attachment B term cannot exceed five years unless approved by the City Council of Customer by ordinance. This Attachment B's termination for any reason will terminate Customer's ability to access Updates, as well as Support and Professional Services.

7.2 Termination by Customer for Convenience. Customer may terminate this Attachment B without cause by providing Zasio with a written termination notice delivered pursuant to this Attachment B's notice requirements.

7.3 Termination for Cause.

7.3.1 Either Party may terminate this Attachment B for the other Party's material breach by written notice (specifying in detail the nature of the breach), effective in 30 days unless the other party first cures the breach, or effective immediately if the breach is not subject to cure.

7.3.2 Upon termination of this Attachment B for cause, Customer's Software license will be terminated, and Customer shall no longer be permitted to use the Software. If this happens, Customer shall provide Zasio with written certification that the original and all copies of the Software, including reports that are generated through the Software, have been completely removed from any server, computer, electronic devices, and any other medium in which the Software and the Software data may be stored, as legally permissible regarding all original and copies of reports.

7.4 Reserved.

7.5 Reserved.

7.6 Limited Survival of Terms. Any obligation under this Attachment B that cannot be performed prior to termination, or that cannot be ascertained until after termination, or which by its nature or intent are to survive, will survive this Attachment B's termination, including, as applicable, Sections 1 (Definitions), 2 (Software License and Restrictions), 3 (Confidential Information), 4 (Data Privacy and Security), 5 (Intellectual Property Rights), 6 (Fees), 8 (Limited Representations, Warranties, and Remedies), 9 (Defense and Indemnification), 10 (Liability Limitations), and 12 (Miscellaneous); Sections 1 (Definition), 3 (Confidential Information), and 6 (Miscellaneous) of the Master Agreement; and Attachment A of the Master Agreement.

8. LIMITED REPRESENTATIONS, WARRANTIES, AND REMEDIES.

8.1 Reserved.

8.2 Software Warranty. Zasio warrants to Customer that the Software will perform substantially in accordance with the pertinent Documentation for a period of 90 days from the date of Customer's receipt.

8.3 Software Warranty Remedy. As Customer's exclusive remedy and Zasio's sole liability for Zasio's breach of its Section 8.2 Software Warranty, Zasio shall correct or replace, at no additional charge, any defective portion of the Software. If Zasio is unable to correct the deficiencies after good-faith efforts and within a commercially reasonable time, Customer may terminate this Attachment B or the applicable Order Form, as appropriate, and Zasio shall refund Customer any fees actually paid by Customer for the defective Software along with any corresponding prepaid fees for Support Services.

8.4 Professional Services and Support Services Warranty. Zasio warrants to Customer that it will perform all Professional Services and Support Services in a professional manner, with a degree of skill and care expected from a skilled and experienced global supplier of substantially similar services, and will devote adequate resources to properly provide Professional Services and Support Services under this Attachment B.

8.5 Professional Services and Support Services Warranty Remedy. As Customer's exclusive remedy and Zasio's sole liability for Zasio's breach of its Section 8.4 Professional Services and Support Services Warranty, Zasio will reperform the Professional Services or Support Services, or both as the case may be, at no additional charge; however, if within a commercially reasonable period Zasio does not cure the defects, Zasio shall refund all fees actually paid by Customer for the defective Services.

8.6 WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS ATTACHMENT B, ALL PRODUCTS AND SERVICES ARE PROVIDED "AS-IS," AND ZASIO HEREBY DISCLAIMS ALL

OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. UNLESS EXPRESSLY DESCRIBED IN THIS ATTACHMENT B OR THE DOCUMENTATION, ZASIO DOES NOT WARRANT THAT ANY PRODUCTS AND SERVICES, OR ANY RESULTS OF THEIR USE, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, OR BE COMPATIBLE WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES.

9. DEFENSE AND INDEMNIFICATION.

9.1 Third-Party Claims Against Customer.

9.1.1 Zasio Obligations. Zasio will indemnify, defend, and hold Customer harmless against any third-party claim against Customer alleging that Customer's use of the Software in accordance with this Attachment B infringes any patent, copyright, or trademark, or misappropriates any trade secret of that third party (each an "IP Claim"). Zasio will indemnify and hold Customer harmless for all damages and costs, including reasonable attorney's fees, finally awarded or paid pursuant to a settlement approved by Zasio, to resolve an IP Claim.

9.1.2 **Zasio's Remedies.** If Customer's use of Software is enjoined as a result of an IP Claim, Zasio may, in its sole discretion:

a. promptly procure Customer's right to continue using the Software;

b. modify or replace the Software so that it is non-infringing, but only if doing so is not harmful to its functional performance, specifications, or use; or

c. if Zasio determines that neither option a. nor b. under this subsection is practical, terminate this Attachment B or any applicable Order Form (as appropriate) and refund Customer for any fees actually paid by Customer for the Software that is the subject of the IP Claim.

9.1.3 **Specific Conditions.** Zasio will have no obligations under this Section 9.1 when the alleged infringement or misappropriation:

a. would not have occurred but for any unauthorized modifications to the Software by Customer or at Customer's direction.

b. arises from Customer's use of the Software not in accordance with this Attachment B or the Documentation;

c. arises from some unauthorized combination by Customer of the Software with any other product, services, or device not provided by Zasio; or

d. arises after Customer receives written notice of termination of any applicable right to use the Software or this Attachment B.

9.2. Third Party Claims Against Zasio. Customer shall defend and hold harmless Zasio against any third-party claim against Zasio alleging a violation or infringement of a User's or third party's rights with respect to Customer Data under this Attachment B.

9.3. Procedures. A Party seeking defense and indemnification under this Section 9 ("**Indemnitee**") shall promptly notify the other Party ("**Indemnitor**") of the claim; however, any failure to give prompt written notice will only relieve an Indemnitor of its obligations under this Section 9 to the extent the failure materially prejudices the Indemnitor's ability to defend the claim. The Indemnitor shall have sole control of the claim's defense and

settlement upon accepting an indemnified claim. An Indemnitee may participate in the claim's defense with its own counsel, at its own expense.

9.4. Remedies. An Indemnitee's remedies in this Section 9 are its sole and exclusive remedy under this Attachment B, and an Indemnitor's entire liability, in connection with any third-party claim under this Section 9.

10. Reserved.

11. Reserved.

12. Reserved.

[*End of Attachment B*]

EXHIBIT 1

PRICING TABLE

Legacy Software

Software	Support Services
Versatile Enterprise Records Management Module Purchased May 29, 2007	Current Support Term through August 31, 2024
Versatile Enterprise Corporate Wide Access Add-On Purchased May 29, 2007	Current Support Term through August 31, 2024
Versatile Enterprise ERMS Module, with 100 count license server Purchased June 5, 2008	Support Term Expired Nov. 30, 2012
Versatile Records On-The-Go Mobile Application Purchased February 25, 2021	Current Support Term through August 31, 2024

New Software

Initial Price

$30,530.00

Price Breakdown

Software	Purchased Plan	One-Time Price
Module: Versatile 2023, On-Premises, with Retention Schedule Management, U.S. Subscription	5-User Pack	$10,995.00
Add-On: Versatile Corporate-Wide Access for Versatile 2023 with Retention Schedule Management, On-Premises	Unlimited Users	$5,995.00
	Subtotal: One-Time Software Price	$16,990.00
Support Services	**Unit**	**Yearly Price**
Annual Maintenance & Support, Versatile 2023, On-Premises, with Retention Schedule Management, U.S. Subscription, 5-User Pack	Annual	$2,995.00
Annual Maintenance & Support, Versatile Corporate-Wide Access for Versatile 2023 with Retention Schedule Management, On-Premises, Unlimited Users	Annual	$1,195.00
	Subtotal: Yearly Maintenance & Support Price	$4,190.00
Professional Services	Unit	One-Time Price
Project Scoping, Management, and Implementation Services	Project	$4,950.00
Integration with Versatile Enterprise, On-Premises	Project	$2,200.00
	Subtotal: One-Time Professional Services Price	$7,150.00
Training (Professional Services)	Hours	One-Time Price
Online Training for Versatile 2023, with Retention Schedule Management ($275/hour)	6	$1,650.00
Online Training for Versatile Corporate-Wide Access ($275/hour)	2	$550.00
	Subtotal: One-Time Training Price	$2,200.00

Project Plan Overview

An optimal Versatile 2023 deployment consists of the following phases. Project timing can vary, but a typical implementation of this scope takes 2 – 3 weeks.

Phase 1: Deployment

Software & Documentation Delivery: Zasio will provide all necessary Versatile Software and user Documentation via email. If needed, Zasio's Support Team can assist your IT staff with installation via telephone and/or remote desktop sharing.

Phase 2: Professional Services

Project Scoping, Management, and Implementation Services: Time estimated for project scoping, tracking, and status calls for the duration of the project implementation.

Data Migration: Has been included in the technical advisory services project which has been quoted separately by Zasio's Consulting Team. If the technical advisory services project does not move forward, a data migration will need to be scoped and priced separately.

Integration: Zasio will integrate the City's new Versatile 2023 with Retention Schedule Management on-prem application with the City's existing Versatile Enterprise on-prem application. Integrating the applications involves creating a link between the two databases such that retention schedule updates completed in the Versatile 2023 with Retention Schedule Management application automatically show in Versatile Enterprise. A Zasio representative will analyze the retention policies of each application and will work with the City's subject-matter experts to determine the best option for linking the data.

Once Versatile Enterprise features (Advanced Records Management) are available in Versatile 2023 on-premises and we're ready to transition Versatile Enterprise on-premises customers, Zasio will notify the City and will estimate the time needed to merge the City's Versatile Enterprise database into the Versatile 2023 database. That project will be quoted separately.

City of San Diego has opted not to include the following items in this project scope and instead these items may be scoped/priced at a later time:

- Test Environment
- Software Validation
- Integration with OpenText
- Integration with SharePoint
- SaaS Deployment

Phase 3: Training

Online Training: Zasio will provide online training for users of the system via GoToMeeting or Microsoft Teams. This allows us to share computer screens so that the trainer can use your database to show functionality and processes. An unlimited number of attendees may attend these sessions and they can also be recorded for future training purposes.

City of San Diego would like access to the software and the ability to start training, while Zasio is working on the technical advisory services project.

EXHIBIT 2

ZASIO ENTERPRISES, INC. SOFTWARE SUPPORT TERMS AND CONDITIONS

These Support Terms and Conditions ("**STCs**") govern the provision of Support Services under the Attachment B. For any conflict between these STC and the Attachment B, the terms of these STCs govern to the extent applicable to the Support Services. Capitalized terms not defined in these STCs are defined in the Attachment B.

1. **SUPPORT SERVICES.** Upon Customer's payment, Zasio shall provide Support Services to Customer on an annual subscription basis.

   1.1 Support Term. A Support Services term is for one year and begins on the date Zasio delivers or makes available the Software to Customer. Following the initial term, the Parties can agree to additional one-year Support Services terms (a "**Support Term**").

   1.2 Reinstatement of Support Services. If Customer does not pay the Support Services fee when due, and does not properly remedy this failure within 30 days of Zasio's written notice, Zasio will terminate Customer's Support Services. However, in Zasio's sole discretion, and subject to Customer's payment of the Reinstatement Fee, Zasio will reinstate Customer's Support Services. "Reinstatement Fee" means payment of the then-current annual Support Service fee plus the prorated amount necessary to make the Support Services continuous from the previous Support Term's expiration if Customer has received the Support Services during the period from the Support Term's expiration.

   1.3 Initiating Support. Customer may contact Zasio for Support Services and any warranty support during Zasio's normal business hours of 7:00 am to 6:00 pm Mountain Time, Monday through Friday, excluding holidays. Zasio's holiday closures for each year may be accessed at http://www.zasio.com/support-services/#supportschedule. If desired, Customer may purchase a subscription to after-hours Support Services at an additional cost.

   1.4 Support Contact Information. Support Services and any warranty support are available via:

   - **E-mail**: support@zasio.com
   - **Toll-free telephone support**: at 1-800-513-1000, option 2.
   - **Remote Desktop Sharing**: If allowed, Zasio's technicians can see exactly what users see on their desktops through remote desktop sharing technology provided by GoToMeeting.com.
   - **Fax**: 208-375-7600. Faxes are placed into a queue the minute they are received and will frequently assist the troubleshooting process, especially where hard-copy reports, labels, or other documents are involved.

2. **SCOPE**. Support Services are focused on maintenance of, and technical support for, the Software. This typically includes diagnosing and fixing errors, as well as identifying enhancements to improve performance and functionality.

3. **CUSTOMER RESPONSIBILITIES**. Support Services are subject to Customer's compliance with the following:

   3.1 Access. Customer shall provide Zasio with necessary access to Customer's Personnel and equipment if a problem Customer is experiencing cannot be reasonably duplicated at Zasio's support facilities.

   3.2 Customer shall document and promptly report to Zasio errors or malfunctions of the Software.

3.3 Customer shall maintain a current backup copy of all Software and related data.

3.4 Customer shall train (or have Zasio train) its end user Personnel in the Software's use and application.

3.5 Customer shall reimburse all reasonable costs incurred by Zasio for any onsite assistance Customer has requested in writing, including travel, boarding, and lodging. Zasio will comply with Customer's then current travel and expense policy when this policy is provided in advance. Any airline travel will be in economy or like class to be eligible for reimbursement.

4. CLASSIFICATION OF ERRORS AND RESPONSE TIME.

CLASSIFICATION	DESCRIPTION	RESPONSE TIME
Fatal Defect	A problem with the Software renders the Software substantially unusable	Zasio will respond with a workaround or plan for resolving the Fatal Defect within one working hour of request. Zasio will dedicate all necessary resources on a priority basis to resolve the Fatal Defect
Material Defect	A problem with the Software that has limited or will limit the Software's use	Zasio will respond with a Workaround or plan for resolving the Material Defect within two business days of request.
Cosmetic Defect	A problem with the Software which impacts a non-essential function while leaving the Software's essential functions intact and operable.	Zasio will fix the Cosmetic Defect in the next regularly scheduled Update.

"**Workaround**" for these STCs means a feasible change in operating procedures so an end-user can avoid the deleterious effects of any defect classification in the table above without material inconvenience.

5. PROVISION OF UPDATES. For current Support Services Customers, Zasio will release Updates approximately every six to twelve months. Updates consisting of maintenance fixes are released on an as needed basis and are available via the Software interface, by download from Zasio's web site, or if requested, by CD/DVD.

6. VERSIONS SUPPORT. Updates provided as part of Support Services include access to the most current major version of the Software. Accordingly, Support Services are available only for the most current major version of the Software, and the immediately preceding major version (except where Support Services are needed to assist Customer with upgrading to the latest Software version). The major version of the Software is identified by the number to the left of the decimal point such as 1.0, 2.0, 3.0, etc., as differentiated from minor releases that are designated by the numbers to the right of the decimal point such as 1.1, 1.2, 1.3, etc.

[End of STCs]

Attachment C: Master Software as a Service and Records and Information Management (RIM) Professional Services Agreement

This Master Software as a Service Agreement (this "**Attachment**" or "**Attachment C**"), effective on the date of the last Party signature on the Master Agreement and approved by the City Attorney ("**Effective Date**"), is between Zasio, and the City of San Diego, a California municipal Corporation ("**Customer**") (individually, a "**Party**" and collectively, the "**Parties**").

This Attachment C establishes the terms for Zasio's provision of Zasio Services (defined below) to Customer, and Customer's access and use of these Zasio Services, for orders placed under this Attachment C. This Attachment C also establishes the terms for Zasio's provision of RIM Professional Services pursuant to a mutually executed Scope of Work ("**SOW**").

1. **Definitions**

These capitalized terms when used in this Attachment C have the following meanings:

"**Add-on**" means any ancillary features and functionality being provided to Customer to support one or more corresponding Modules (such as the Versatile Notification System or Versatile Import Utility Add-ons).

"**Change**" means any change to Zasio Services that would materially alter the scope, parameters, or schedule for delivery of Zasio Services.

"**Customer Systems**" means Customer's information technology infrastructure (such as its computers, software, hardware, databases, applications, and electronic and database management systems and networks), whether operated directly by Customer or through its third-party service providers and sub-processors.

"**Documentation**" when used in this Attachment C means Zasio's user and technical documents that Zasio makes available to Customer under this Attachment C and which describe the Hosted Services' functionality, components, features, configuration, use, support, maintenance, and requirements.

"**Emergency Downtime**" means any period during which the Hosted Services are down resulting from emergency or critical maintenance that is required to maintain the security or performance of the Hosted Services or Hosting Facility's network or infrastructure. Zasio will use best efforts to provide advance notice of Emergency Downtime but cannot guarantee advance notice.

"**Hosting Facility**" means the cloud vendor (including its applicable data center[s]) that Zasio has selected to provide network and computing infrastructure through which the Hosted Services and related Customer Data storage are provided.

"**Hosted Services**" collectively means the Modules, Purchased Plans, and Add-ons identified in an Order Form that Zasio provides to Customer (i) as a hosted application; and (ii) on a subscription basis. Hosted Services include related Documentation and Updates. Any additional terms applicable to subsequent Hosted Services subscriptions purchased under this Attachment C will be identified in the applicable Order Form.

"**Information Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Data on systems managed or otherwise controlled by Zasio.

"**Internal Business Use**" when used in this Attachment C means Customer's access and use of Zasio Services for Customer's own internal business operations. Internal Business Use does not include Customer's access and use of Zasio Services to provide services to any third party or in a manner that is competitive to Zasio.

"**Module**" means each major bundle of related Hosted Services features and functionality that Zasio provides to Customer, such as retention schedule management or physical records management.

"**Pricing Table**" when used in this Attachment C means the document forming part of this Attachment C as **Exhibit 1.** The Pricing Table establishes the details and pricing information for the Zasio Services that Customer is initially purchasing under this Attachment C.

"SaaS **Professional Services**" when used in this Attachment C means optional implementation, on-site or remote training, configuration, integrations, data migration, and similar services provided by Zasio. Any SaaS Professional Services that Customer purchases will be reflected in the applicable Order Form. Unless expressly stated otherwise in the applicable Order Form, SaaS Professional Services may be invoiced at their then current rate if not requested within 1 year of the applicable Order Form's effective date.

"**Prohibited Data**" means sensitive personal information, special category data, or like terms defined under applicable data privacy laws; government-issued identification numbers; personal health information; account passwords or security information; financial account information; payment information, individual credit or income information, or data or information that imposes specific data security or data protection obligations on Zasio that are in addition to or different from those obligations specified in this Attachment C.

"**Purchased Plan**" means the category of access for each Module (such as the number of authorized users or jurisdictional scope of citations).

"**Scheduled Downtime**" for the Hosted Services includes the periods during which the Hosted Services will not be available due to the following work being performed by Zasio or the Hosting Facility: (a) modification or repairs to shared infrastructure, such as core routing or switching infrastructure that occurs during off peak hours (where possible) in the time zone where the Hosting Facility's data center is located; or (b) maintenance of a custom configuration that Customer requests and Zasio has scheduled in advance (either on a case-by-case basis or based on standing instructions).

"**Service Level Guarantee**" means **Exhibit 3**, which forms part of this Attachment C and establishes Zasio's guarantee to Customer concerning Hosted Services' availability.

"**Subscription Term**" means Customer's prepaid initial and any renewal subscription period for Customer's access and use of the corresponding Hosted Services. Each prepaid subscription period will be one year unless the Parties agree to a different period in an Order Form (or where appropriate, an accepted Renewal Document), but will in all cases end on the date that the applicable Hosted Services are canceled, the applicable Hosted Services subscription ends, or this Attachment C or any corresponding Order Form is terminated pursuant to the terms of this Attachment C.

"**Support Services**" when used in this Attachment C means Zasio's standard services to maintain and support the Hosted Services, including the provision of Updates, provided as part of Customer's Hosted Services subscription. Support Services are described in more detail in Zasio's Support Services Terms, which form part of this Attachment C as **Exhibit 2**.

"**Updates**" when used in this Attachment C means modifications, additions, or adjustments to any specific solution forming part of the Hosted Services, and which Zasio has developed to (i) correct bugs, deficiencies, or errors; (ii) conform to regulatory or industry requirements; or (iii) incorporate improvements in operability. An Update does not include a separate product or service, provided under different terms, consisting of substantially different architectural features and functionality (even if such a product or service shares some common functionality with its predecessor).

"**Usage Data**" means data and information that relates to Hosted Services operation, use, performance, and availability, including patterns identified through the use of Hosted Services and log data.

"**User**" means an employee, independent contractor, or other agent of Customer that Customer has authorized to access and use the Hosted Services on its behalf in support of Customer's Business Operations.

"**Zasio Services**" means the Hosted Services, Support Services, and any SaaS Professional Services in an Order Form that Zasio provides to Customer under this Attachment C. If the Parties include the RIM Professional Services Terms as an exhibit to this Attachment C, RIM Professional Services (as defined in Exhibit 5, the RIM Professional Services

Terms) will also be considered Zasio Services, and fees for Professional Services must be set forth in the applicable statement of work.

"**Zasio RIM Professional Services Supplemental Terms**" (the "RIM **Professional Services Terms**") means the additional terms and conditions applicable to Zasio's provision of Consulting Services to Customer, which form part of this Attachment C as **Exhibit 5**.

2. HOSTED SERVICES

2.1 **Provision of Hosted Services.** During the Subscription Term, Zasio grants Customer a limited, non-exclusive, non-transferable (except in accordance with Master Agreement Section 6.1 (Assignment)), non-sublicensable, royalty-free right to access and use the Hosted Services in scope for the Purchased Plan, as well as any related Zasio Materials disclosed to Customer, in accordance with this Attachment C and solely for Customer's Internal Business Use. Customer may access and use Hosted Services and any Zasio Materials worldwide, subject to any restrictions pursuant to Master Agreement Section 6.4 (Export Control Obligations), this Attachment C's Section 3 (Customer Obligations and Restrictions), and Zasio's termination for cause rights in Section 8.3 of this Attachment C.

2.2 **Competitive Users.** Customer shall ensure that all Users are bound by confidentiality terms at least as protective as the confidentiality terms in the Master Agreement.

2.3 **Customer Access and Use.** Customer's Hosted Services access will cease upon this Attachment C's or an applicable Order Form's termination, the termination or non-renewal of a corresponding Subscription Term, or the suspension or termination of Customer's access in accordance with this Attachment C.

2.4 **Support Services.** During the Subscription Term, Zasio shall provide Customer with Support Services in accordance with the Support Services Terms.

2.5 **Mobile Applications.** Zasio may make available to Customer a mobile application to download and utilize in connection with certain Hosted Services. The use of any mobile application provided by Zasio will be governed by any terms and conditions presented upon downloading or otherwise receiving access to the mobile application.

2.6 **Access Date.** Unless the Parties agree differently in writing, Customer's access to the Hosted Services identified in the Pricing Table will begin no later than 5 business days after this Attachment C's Effective Date or, for subsequently-purchased Hosted Services, the date the Parties enter into the related Order Form (the "**Access Date**"). The Access Date will mark the first day of Customer's Subscription Term for the corresponding Hosted Services.

2.7 **Hosted Database.** Customer is limited to one database instance per Hosted Services subscription unless the Parties expressly agree otherwise in writing.

2.8 **Hosted Service and System Control.**

2.8.1 **Zasio's Responsibilities.** Zasio has sole control over the operation, provision, maintenance, and management of the Hosted Services, including the:

a. systems and applications used to host the Hosted Services;

b. selection, deployment, modification, and replacement of the Hosted Services; and

c. maintenance, upgrades, Updates, corrections, and repairs to the Hosted Services.

2.8.2 **Modifications.** Zasio may make changes to the Hosted Services (including maintenance and upgrade windows) to maintain or enhance Hosted Services (i) quality; (ii) delivery; (iii) market strength; (iv) cost efficiency; or (v) performance.

This may include replacing functionality with a functional equivalent or removing functionality where the removal does not materially degrade core functionality. If a change materially degrades overall functionality, Customer may terminate its subscription to the corresponding Hosted Services by providing written notice within 45 days. Zasio will provide reasonable notice before any functionality change.

2.8.3 **Suspension of Hosted Services.** Zasio may suspend or limit Customer's Hosted Services access without liability if Customer uses the Hosted Services:

a. beyond the scope of Customer's rights under this Attachment C; or

b. in a manner that Zasio reasonably believes poses an immediate threat to the availability or security of the hosted systems or Hosting Facility (such as by introducing a virus to the hosted system).

Zasio will promptly notify Customer of any suspension or limitation, and will limit the time and scope as reasonably appropriate.

2.8.4 **Hosted Services Disclaimer**. Zasio does not promise that the Hosted Services will be uninterrupted, error free, or completely secure. Customer acknowledges and agrees that there are risks inherent in internet connectivity that could result in the loss of, or damage to, privacy, Customer Data, Confidential Information, or property in connection with Customer's access and use of Hosted Services.

2.8.5 **Hosting Facility Disclaimer.** Zasio has selected a Hosting Facility in the United States that is compatible with the Hosted Services, but may transition to another Hosting Facility in the United States. Customer Data stored on Zasio's internal systems and servers will also be stored in the United States. During a Subscription Term, Zasio will provide at least 30 days' advance written notice of any Hosting Facility change. Any new Hosting Facility will not result in material degradation to the protections and security required under this Attachment C. Zasio will not engage any Hosting Facility without including contractual terms that are at least as protective as the Master Agreement and its attachments.

2.9 **Usage Data.** Zasio may collect, process, and disclose Usage Data (i) to monitor and protect the security of the hosted system; or (ii) so that it may improve and enhance the Hosted Services. Should Zasio disclose any Usage Data to a third party, it will be aggregated and anonymized to avoid identifying Customer or any User.

2.10 **Usage Limit.** Customer's data storage limit is 20 GB across all Hosted Services, unless an Order Form or an accepted Renewal Document provides for greater storage. Customer's storage limit does not include backups, operating systems, and software required to run the hosted system. If Customer exceeds a contractual usage limit, additional data fees may apply; Zasio will work in good faith with Customer, however, to reduce Customer's usage to be below the limit before applying any additional fees.

2.11 **Change Control Procedures.** The Party requesting a Change must give written notice to the other Party's designated individual. The request must detail the Change and the reasons for it. The Parties shall negotiate in good faith any Change, including any related revised fees. Prior to implementing a Change, the Parties shall execute a change order detailing the Change and any modified terms.

2.12 **On-Premises Software.** Certain configurations of Hosted Services may require installation of Zasio On-Premises Software on Customer's systems (**"On Premises Software"** means those programs and applications in object code form identified in an Order Form for Hosted Services, and which are licensed to Customer for installation on Customer Systems for the duration of any corresponding term for Support Services). Any applicable On-Premises Software will be further described in the appropriate Order Form. Upon execution of an applicable Order Form, Zasio grants Customer a limited, non-exclusive, non-transferable (except in accordance with Section 6.1 (Assignment) of the Master Agreement), non-sublicensable license to install and use the On-Premises Software for Customer's Internal Business Use in conjunction with the corresponding Hosted Services. When On-Premises Software is licensed to Customer, and subject to this Section 2.12, the

term Hosted Services shall include any corresponding On-Premises Software; however, additional fees may be identified in the Order Form for the licensing of On-Premises Software as well as any related subscription to Support Services.

3. CUSTOMER OBLIGATIONS AND RESTRICTIONS

3.1 **Prohibited Conduct**. Customer shall not, and shall not permit its Users or any other party to:

a. copy, modify, reverse engineer, decompile, disassemble, seek or obtain the source code, or create derivative works or improvements of any Hosted Services;

b. transmit or store in the Hosted Services any Prohibited Data. To the extent Customer uses Hosted Services for the transmission or storage of Prohibited Data, Customer does so entirely at its own risk;

c. make any Zasio Services available to any other party (such as by renting, leasing, lending, selling, licensing, sublicensing, assigning, distributing, publishing, transferring, or otherwise) unless expressly authorized elsewhere in the Master Agreement (such as pursuant to Master Agreement Section 6.1 (Assignment) or this Attachment C's Section 3.2.1 (Users));

d. access or use the Hosted Services or any Zasio Materials to build a competitive product or service or to copy any ideas, features, functions, or graphics of the Hosted Services;

e. access or use the Hosted Services to engage in or promote illegal, abusive, exploitative, malicious, or repugnant behavior;

f. access or use the Hosted Services for the purpose of interfering with the shared system's operations or resources; or

g. use any Zasio Services in violation of this Attachment C.

Customer is responsible for all activities conducted by or through it with respect to the Hosted Services or any Zasio Materials.

3.2 **Customer Responsibilities**

3.2.1 **Users**. Customer may designate Users and permit Users to access and use Zasio Services in accordance with this Attachment C. Access credentials for the Hosted Services may not be accessed or used by more than one individual, but may be transferred from one individual to another if the original User is no longer permitted by Customer to access or use the Hosted Services.

3.2.2 **Responsibilities**. Except for Zasio's responsibilities described in Section 3 of the Master Agreement (Confidential Information) and Section 4 of this Attachment C (Data Security and Processing), Customer has sole responsibility for:

a. the accuracy, quality, and legality of Customer Data;

b. the security and confidentiality of its account information; and

c. preventing unauthorized access or use of its Hosted Services subscription, and promptly notifying Zasio of any such unauthorized access or use.

3.2.3 **Customer Systems**. Customer retains control over the operation, maintenance, management, and use of Customer Systems that are used to access the Hosted Services.

3.2.4 **Harmful Code**. Customer shall not introduce or transmit through the Hosted Services any virus, worm, or other harmful code.

3.2.5 **Cooperation**. Upon Zasio's reasonable request, Customer must reasonably assist Zasio to enable Zasio to perform its obligations under this Attachment C. Zasio is not responsible for any delay or failure of its performance caused by Customer's failure to promptly perform Customer's obligations under this Attachment C.

3.2.6 **Security Standards**. Customer will maintain reasonable security standards for its Users' use of Hosted Services, including establishing adequate physical security and environmental controls of all devices accessing Hosted Services.

3.2.7 **Legal Compliance**. Customer must comply with all applicable laws and regulations in connection with its access and use of the Hosted Services, collection and other processing of Customer Data, and performance under this Attachment C. Customer acknowledges and agrees that Zasio has no control over the Customer Data transmitted by or on behalf of Customer through Hosted Services and no obligation to independently verify or examine the accuracy, quality, and legality of Customer Data.

3.2.8 **Proprietary Notices**. Customer shall not remove, alter, or obscure any of Zasio's copyright, trademark, trade name, or other property right notices from any Zasio Services, including Zasio Materials.

4. DATA SECURITY AND PROCESSING FOR HOSTED SERVICES

4.1 **Zasio's Security Program**. Zasio will maintain appropriate administrative, physical, and technical safeguards designed to protect Customer Data security, integrity, and confidentiality, including measures designed to prevent the unauthorized access, use, modification, or disclosure of Customer Data. Zasio's current information security program applicable to the Hosted Services is described in the Technical and Organizational Measures, which form part of this Attachment C as **Exhibit 4**. Zasio will operate in conformance with these Technical and Organizational Measures, as well as the measures and protocols regarding data security for the Hosted Services as set forth in Zasio's most current SOC 2, Type 2 (or equivalent) report, which Zasio will make available to Customer upon request. The Technical and Organizational Measures are subject to technical progress and development, and Zasio may modify them from time to time provided that doing so does not materially degrade the Hosted Services' overall security. Any material updates to Zasio's Technical and Organizational Measures will be communicated to Customer through (i) email; or (ii) Zasio's Customer Service Portal. Zasio's Technical and Organizational Measures, in conjunction with Zasio's security commitments elsewhere in this Attachment C, are Zasio's only responsibility with respect to Customer Data. Customer is responsible for making an independent determination of whether the Technical and Organizational Measures (i) are appropriate to Customer Data and Zasio Services; and (ii) meet Customer's requirements and security obligations, including any applicable City of San Diego Administrative Regulations. To assist with Customer's independent determination, Zasio understands and agrees that it will comply with the City's IT Governance review processes in effect at that time.

4.2 **Customer Personal Data**. The only kind of Personal Data that Zasio requires to provide Zasio Services under this Attachment C is Personal Data (i) of Customer Personnel commonly known as business contact information (such as name, job title, employer, business email address, business telephone number, and the like); and (ii) consisting of limited bank and payment card details related to payment under this Attachment C. Customer shall use commercially reasonable efforts to minimize any transfer of Personal Data to Zasio to that appropriate to the Hosted Services Customer purchases under this Attachment C. Customer has sole responsibility to notify Zasio if Customer believes that Customer Data provided to Zasio under the Attachment C becomes subject to any privacy, security, or other legal requirements not incorporated into this Attachment C. If this happens, the Parties shall work in good faith to include the additional requirements in an amendment.

4.3 **Limited Use of Personal Data.** For purposes of the California Consumer Privacy Act ("CCPA"), Zasio is a service provider and Customer is a government entity and Zasio shall comply with all obligations applicable to a service provider, including those related to Personal Data privacy and security. Zasio shall not sell or share Personal Data (as those terms are defined under the CCPA, regardless of the CCPA's application). Zasio also shall not retain, use, or disclose Personal Data outside of the direct business relationship between Zasio and Customer or for a commercial purpose (as that term is defined in the CCPA). Zasio's access to any Personal Data is not part of the consideration exchanged in respect of this Attachment C.

4.4 **Legal Rights to Personal Data.** If anyone contacts Zasio to exercise a legal right with respect to Personal Data, Zasio shall promptly forward the request to Customer and shall not respond except to inform the individual of this. Zasio shall promptly and reasonably assist Customer to fulfil any individual request to exercise their rights under applicable data privacy law, including a request to access, delete, opt-out, or receive information about the processing of Personal Data pertaining to them. Notwithstanding the foregoing, Zasio acknowledges and agrees that Customer is not a business under the CCPA and is not subject to the obligations of a business under the CCPA. Customer has sole responsibility to notify Zasio if Customer believes that Personal Data provided to Zasio under this Attachment C becomes subject to any privacy or security requirements from jurisdictions that are not incorporated into this Attachment C. If this happens, the Parties shall work in good faith to include the additional requirements in an amendment.

4.5 **Customer Data Entry.** Unless Zasio expressly agrees to enter Customer Data into the Hosted Services as part of providing SaaS Professional Services pursuant to an Order Form, data entry is Customer's responsibility. In either event, between the Parties, Customer remains the exclusive owner of all rights in Customer Data. Customer grants Zasio a non-exclusive, limited right to process and use Customer Data to provide Zasio Services in accordance with this Attachment C.

4.6 **Penetration Tests.** Customer shall not conduct or authorize any penetration testing of the Hosted Services or any of Zasio's systems without Zasio's express written approval. This includes (i) probing, scanning, penetrating, or testing a Hosted Services' or a related system's or network's vulnerability; or (ii) breaching any security measures, whether by passive or intrusive techniques.

4.7 **Retention and Destruction.** In addition to Zasio's express and limited rights to retain Customer Data under this Attachment C, Zasio may retain Customer Data to comply with applicable laws and Zasio's disaster recovery process. Zasio's retention and use of Customer Data must be in accordance with Section 3 of the Master Agreement (Confidential Information).

4.8 **Backups.** For each Customer database and dedicated server in the Hosting Facility, Zasio performs: (i) an automatic, daily, point-in-time-restore (hot) backup, which is retained for two weeks; and (ii) a monthly backup, which is retained for three months. Zasio Services, however, do not replace Customer's need to maintain regular backups, redundant data archives, or exports of up-to-date hosted Customer Data. The Service Level Guarantee (including the Recovery Point Objective) is Customer's sole and exclusive remedy and Zasio's entire liability for any loss, alteration, destruction, damage, corruption, or recovery of Customer Data within the Hosted Services database that results from a server or database failure.

4.9 **Return of Hosted Customer Data.**

4.9.1 At any time during a Subscription Term, Customer may use the Hosted Services' built-in reporting and exporting functions to export Customer's previously uploaded Customer Data (the "**Customer Database**").

4.9.2 If Customer requires additional time to retrieve its Customer Database, Customer shall have up to 60 days following the end of the applicable Subscription Term to extract Customer Data and any other data that Customer deems necessary. Upon receipt, Zasio, without additional charge, will preserve Customer's ability to export its Customer Database for an additional 30 days past the end of the applicable Subscription Term (a "**Transition Period**").

4.9.3 Upon Customer's written request received before the end of a Subscription Term, or where applicable, a Transition Period, and for an additional reasonable fee in accordance with the Pricing Table Zasio will also provide Customer with the following SaaS Professional Services: (i) an export of its Customer Database in flat file format via secure file transfer method; (ii) reasonable technical assistance exporting its Customer Database; (iii) reasonable technical assistance to help Customer understand its Customer Database; or (iv) some or all of these things (**"Transition Assistance"**).

4.9.4 At the end of a Subscription Term, Transition Period, or data extraction period set forth in Section 4.9.2 above, Zasio shall have no other obligations to maintain or provide a Customer Database or provide Transition Assistance, and unless legally prohibited, shall thereafter delete the Customer Database.

4.9.5 Zasio is not required to remove Usage Data from Zasio's log systems, or copies of Customer Data from Zasio's backups, prior to the time that these are scheduled for deletion under Zasio's log data and backup and recovery policies. Zasio is also not obligated to delete any information or records related to Customer account management prior to deletion in the normal course under Zasio's records retention schedule.

4.10 **Incident Notification**. Upon becoming aware of any Information Security Incident, Zasio will notify Customer without undue delay and in accordance with applicable law. Zasio will promptly investigate the cause of the Information Security Incident, seek to mitigate its consequences, and seek to prevent a recurrence. As information becomes available, Zasio will promptly inform Customer of (i) the nature and reasonably anticipated consequences of the Information Security Incident; (ii) Zasio's mitigation measures and efforts to prevent a recurrence; (iii) where possible, information about the types of Customer Data that were the subject of the Information Security Incident; and (iv) any other information required by applicable law. Zasio's obligations under this Section 4.10 shall not be an acknowledgment by Zasio of any fault or liability in connection with the Information Security Incident.

5. Reserved.

6. INTELLECTUAL PROPERTY RIGHTS

In accordance with this Attachment C's Section 2.1 (Provision of Hosted Services), Customer only obtains a limited right to access and use the Hosted Services under this Attachment C. Zasio retains all other rights in the Hosted Services and Zasio Materials, including all related intellectual property rights.

7. SUBSCRIPTION AND ATTACHMENT C TERM

7.1 **Subscription Term.** The Subscription Term for any Hosted Services will begin on its corresponding Access Date.

7.2 **Renewal Term.** Approximately 45 days before the end of a Subscription Term, Zasio will invoice Customer to renew the Subscription Term (or Upon Customer's request, provide a renewal notice in lieu of a renewal invoice) (each, a **"Renewal Document"**). Customer may accept a Renewal Document by timely paying the fees for Zasio Services reflected in the Renewal Document.

7.3 **Attachment C Limited Survival of Terms.** Attachment C's termination for any reason will terminate Customer's ability to access and Use Hosted Services. Any obligation under this Attachment C that cannot be performed prior to termination, or that cannot be ascertained until after termination, or which by its nature or intent are to survive, will survive this Attachment C's termination, including, as applicable, Sections 1 (Definitions), 3.1 (Prohibited Conduct), 4 (Data Security and Processing), 6 (Intellectual Property Rights), 9 (Payment), 10 (Limited Representations, Warranties, and Remedies), 11 (Defense and Indemnification), 12 (Liability Limitations), and Sections 1 (Definition), 3 (Confidential Information) and 6 (Miscellaneous) of the Master Agreement.

8. TERMINATION

8.1 **Reserved.**

8.2 **Customer's Termination for Convenience.** Customer will receive a refund of any prepaid fees for the pro rata share of any unused Subscription Term.

8.3 **Termination.** A Party may terminate this Attachment C:

a. for cause 30 days after the other Party's receipt of written notice of that other Party's material breach of this Attachment C (including Customer's failure to timely pay any money due within 30 days of its due date), unless the breaching party has cured the breach during the 30-day period;

b. for cause immediately upon written notice if the material breach is not subject to cure.

c. immediately for cause upon the other Party's breach of its obligations under Master Agreement Sections 3 (Confidential Information), 6.4 (Export Control Obligations), or 6.1 (Assignment), or Customer's breach of this Attachment C's Section 3.1 (Prohibited Conduct).

8.4 **Obligations Upon Termination.** Except as provided under Section 4.9 of this Attachment C, Zasio will disable Customer's access to applicable Hosted Services upon the end of a corresponding Subscription Term, and Customer shall immediately cease its access and use of the terminated Hosted Services.

8.5 **Limited Return of Fees.** Upon Customer's termination of this Attachment C or any Subscription Term for Zasio's material breach pursuant to Section 8.3(a), (b), or (c) of this Attachment C, Zasio will provide a pro rata refund to Customer of any fees paid by Customer to Zasio for the remainder of any terminated Subscription Term. Any fees for Zasio Services rendered prior to termination will remain due.

9. PAYMENT

9.1 **Invoicing.** Zasio will invoice Customer for the initial Hosted Services subscription period following the Access Date. Zasio will invoice Customer for SaaS Professional Services and any reimbursable out-of-pocket expenses the calendar month after they are incurred. Zasio will invoice reimbursable out-of-pocket expenses (including travel, lodging, and meals) in accordance with Customer's reasonable travel and expense policy.

9.2 **Reserved**

9.3 **Fees.**

a. all fees are stated in and must be paid in U.S. dollars.

b. all fees for Customer's initial purchase of Zasio Services under this Attachment C will be stated in the Pricing Table. Fees for any subsequently-ordered Zasio Services will be stated in the applicable Order Form. Fees for any renewal Subscription Term will be stated in the applicable Renewal Document. Zasio will limit any fee increase for a Subscription Term renewal to 4 percent, per annum. However, Zasio reserves the right to additionally increase Hosted Services fees as they are increased by the Hosting Facility. Fees for any subsequently-ordered SaaS Professional Services will be at Zasio's then-existing standard rate unless the Parties expressly agree otherwise in writing.

9.4 **Late Payment**. If any fees not subject to reasonable dispute remain unpaid by their due date, in addition to any other rights or remedies Zasio may have by law or under this Attachment C:

b. Zasio may suspend Customer's Hosted Services access and use upon 30 days' written notice, and until the amounts are paid in full;

c. Reserved.

d. Reserved.

9.5 Reserved.

10. LIMITED REPRESENTATIONS, WARRANTIES, AND REMEDIES

10.1 Reserved.

10.2 **Hosted Services Warranty**. Zasio warrants to Customer that (i) it will comply with all laws applicable to its performance of its obligations under this Attachment C, and (ii) the Hosted Services will perform substantially in conformance with the Documentation. Subsection (ii) of this warranty will only apply if Customer has utilized the applicable Hosted Services in material accordance with the Documentation, this Attachment C, and applicable law.

10.3 **Hosted Services Warranty Remedy.** As Customer's exclusive remedy and Zasio's sole liability for Zasio's breach of its Section 10.2 Hosted Services Warranty, Zasio shall: (a) correct the non-conformity at no additional charge; or (b) if Zasio is unable to correct the non-conformity after good-faith efforts and within a commercially reasonable time, Customer may terminate the non-conforming Hosted Services or this Attachment C, or both, and Zasio shall refund Customer a pro rata portion of the prepaid subscription fees paid by Customer for the defective Hosted Services.

10.4 **SaaS Professional and Support Services Warranty**. Zasio warrants to Customer that it will perform all SaaS Professional Services and Support Services in a professional manner, with a degree of skill and care expected from a skilled and experienced global supplier of substantially similar services, and will devote adequate resources to properly provide SaaS Professional Services and Support Services under this Attachment C.

10.5 **SaaS Professional and Support Services Remedy**. As Customer's exclusive remedy and Zasio's sole liability for Zasio's breach of its Section 10.4 SaaS Professional Services and Support Services Warranty, Zasio shall: (a) correct any deficiencies in SaaS Professional Services or Support Services at no additional charge; or (b) if Zasio is unable to correct the deficiencies after good-faith efforts and within a commercially reasonable time, (i) Customer may terminate the corresponding Hosted Services or this Attachment C; (ii) Zasio shall refund Customer the fees paid by Customer for the defective services; and (iii) Zasio shall provide Customer a pro rata refund (from the date of termination) of any subscription fees paid by Customer for the terminated Hosted Services.

10.6 **Notice of Termination**. Customer must provide any notice of termination under this Section 10 within 30 days of Zasio's failure to correct the corresponding deficiencies.

10.7 **WARRANTY DISCLAIMER**. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS SECTION 10, ALL ZASIO SERVICES ARE PROVIDED "AS IS," AND ZASIO HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. UNLESS EXPRESSLY DESCRIBED IN THE DOCUMENTATION, ZASIO DOES NOT WARRANT THAT ANY ZASIO SERVICES OR ANY RESULTS OF THEIR USE WILL MEET CUSTOMER'S OR ANY OTHER PARTY'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, OR BE COMPATIBLE WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES.

11. DEFENSE AND INDEMNIFICATION

11.1 **Third-Party Claims Against Customer.**

11.1.1 **Zasio's Obligations.** Zasio will defend and hold harmless Customer against any third-party claim against Customer alleging that Customer's use of Hosted Services in accordance with this Attachment C directly infringes any patent, copyright, or trademark, or misappropriates any trade secret of that third party (each an "**IP Claim**"). Zasio will indemnify and hold harmless Customer for all damages and costs, including reasonable attorney's fees, finally awarded or paid pursuant to a settlement approved by Zasio, to resolve an IP Claim.

11.1.2 **Zasio's Remedies.** If Customer's access and use of any Hosted Services is enjoined as a result of an IP Claim, Zasio may, in its sole discretion:

d. promptly procure Customer's right to continue using the Hosted Services;

e. modify or replace the Hosted Services so that they are non-infringing, but only if doing so is not harmful to their functional performance, specifications, or use; or

f. if Zasio determines that neither option a. nor b. under this subsection is practical, terminate this Attachment C or any applicable Order Form (as appropriate) and refund Customer the prorated amount for any fees actually paid by Customer for the Hosted Services that are the subject of the IP Claim.

11.1.3 **Specific Conditions.** Zasio will have no obligations under this Section 11 when the alleged infringement or misappropriation:

a. would not have occurred but for any unauthorized modifications to Hosted Services by Customer or at Customer's direction;

b. arises from Customer's use of Hosted Services not in accordance with this Attachment C or the Documentation;

c. arises from some unauthorized combination by Customer of access or use of the Hosted Services in combination with any other product, services, or device not provided by Zasio; or

d. arises after Customer receives written notice of termination of any applicable right to access and use the Hosted Services or this Attachment C.

11.2 **Third-Party Claims Against Zasio.** Customer shall defend and hold harmless Zasio against any third-party claim against Zasio (including Zasio's subcontractors) alleging a violation or infringement of a User's or third party's rights with respect to Customer Data under this Attachment C.

11.3 **Procedures.** A Party seeking defense and indemnification under this Section 11 ("**Indemnitee**") must promptly notify the other Party ("**Indemnitor**") of the claim; however, any failure to give prompt written notice will only relieve an Indemnitor of its obligations under this Section 11 to the extent the failure materially prejudices the Indemnitor's ability to defend the claim. The Indemnitor shall have sole control of the claim's defense and settlement upon accepting an indemnified claim. An Indemnitee may participate in the claim's defense with its own counsel, at its own expense.

11.4 **Remedies.** An Indemnitee's remedies in this Section 11 are its sole and exclusive remedy, and an Indemnitor's entire liability, in connection with any third-party claim under this Section 11.

12. Reserved.

13. Reserved.

14. Reserved.

Exhibit 1

Pricing Table

[No Pricing Table as of Agreement Effective Date. The Parties Will Complete Any Subsequent Hosted Services Transaction Via a Mutually Executed Order Form]

Exhibit 2

Support Services Terms

These Support Services Terms ("**SSTs**") govern Zasio's provision of Support Services under Attachment C. For any conflict between these SSTs and Attachment C, these SSTs will govern to the extent applicable to Support Services. Capitalized terms not defined in these SSTs are defined in Attachment C.

1. **AVAILABILITY AND CONTACT INFORMATION**

1.1 Hours. Customer may contact Zasio for support during Zasio's normal business hours of 7:00 am to 6:00 pm, Mountain Time, Monday through Friday, excluding holidays. Zasio's holiday closures for each year are available at http://www.zasio.com/support-services/#supportschedule.

1.2 Methods of Contact. Customer can request support via: 1.) email at ZasioSupport@zasio.com; 2.) phone at (800) 513-1000 (option 2); or 3.) through Zasio's online customer portal (and access information will be provided to Customer at the time of the Access Date).

1.3 Remote Desktop Sharing: If Customer permits, Zasio's technicians can see exactly what Users see on their desktops through remote desktop sharing technology.

2. **SUPPORT SERVICES**

2.1 Scope. Support Services are focused on maintenance of, and technical support for, the software accessed through the Hosted Services. This typically includes diagnosing and fixing errors, as well as identifying enhancements to improve performance and functionality.

2.2 Party Obligations. Zasio will make all commercially reasonable efforts to correct or offer a Workaround (defined below) or plan for Customer-identified defects which Zasio has validated. To enable Zasio's provision of Support Services, Customer shall:

i. Provide Zasio with access to all appropriate Customer personnel;

ii. Document and report Hosted Services errors or malfunctions within 72 hours; and

iii. Ensure all Users are properly trained in the use and application of the Hosted Services.

2.3 Response Time.

2.3.1 Zasio shall respond to Support Services requests as follows:

CLASSIFICATION	DEFINITION	RESPONSE TIME
Fatal Defect	A problem with the software that renders the software substantially unusable.	Zasio will respond with a Workaround or plan for resolving the Fatal Defect within one business hour of the request. Zasio will dedicate all necessary resources on a priority basis to resolve the Fatal Defect
Material Defect	A problem with the software that has limited or will limit the software's use.	Zasio will respond with a Workaround or plan for resolving

		the Material Defect within two business days of the request.
Cosmetic Defect	A problem with the software that impacts a non-essential function while leaving the software's essential functions intact and operable.	Zasio will fix the Cosmetic Defect in the next regularly scheduled Update.

2.3.2 **"Workaround"** for these SSTs means a feasible change in operating procedures where an end-user can avoid the deleterious effects of any defect classification, as defined in the table above, without material inconvenience.

2.4 **Updates.** Updates to the software forming part of the Hosted Services are provided to customers who are within a Subscription Term. Updates will be applied as soon as practical upon becoming available, and with at least 24 hours' notice (except emergency operating system patches). Updates will be applied in the following manner:

2.4.1 **Operating System Patches:** Regular patches to the Hosted Services' operating system are applied at regularly occurring, predetermined intervals, usually once per calendar month. Emergency operating system patches will be applied as needed and, where practicable, with 24 hours' notice.

2.4.2 **Critical Software Updates**: Will be applied as soon as practicable upon becoming available, usually after midnight (in the location of the Hosting Facility) following the day of release.

2.4.3 **Non-Critical Software Updates**: Including improvements to the software package, will be provided approximately every 6 to 12 months. Advance notice and release notes will precede these Updates.

2.4.4 **Database Updates**: Upon approval by Customer.

[End of SSTs]

Exhibit 3

Zasio Service Level Guarantee

1. **Scope and Applicability**. This Service Level Guarantee ("**SLG**") describes Zasio's guarantee to Customer concerning Hosted Services Availability and forms part of the Parties' Attachment C. Upon any conflict between this SLG and Attachment C, the terms of this SLG will prevail with respect to Hosted Services Availability. Capitalized terms not defined in this SLG are defined in Attachment C or the Master Agreement.

2. **Guarantee**. For the provision of Hosted Services, the Hosting Facility will host Zasio software and related Customer Data at a data center in the United States chosen by the Hosting Facility. "**Hosted Services Availability**" is defined as the Hosted Services being available to Customer without material access errors during the Subscription Term. Zasio guarantees 99.5% Hosted Services Availability during any given calendar month, excluding periods of: (a) application of Updates; (b) Scheduled Downtime; (c) Emergency Downtime; (d) unavailability due to Customer error; (e) Force Majeure Event that prevents access to the Hosted Services; or (f) suspended access due to Customer's use of the Hosted Services in violation of this SLG or Attachment C. Unless one of these express exceptions applies, Hosted Services Availability below 99.5% during any calendar month constitutes a "**Service Level Failure**."

3. **Downtime Measurement**. A Service Level Failure is measured from the time Customer attempts but is unable to access Hosted Services until Hosted Services Availability is restored. To receive a Service Level Credit (defined in the Service Level Credit table below), Customer must make reasonable efforts to promptly notify Zasio of any lack of Hosted Service Availability so that it can be restored as soon as possible. Periods of Scheduled Downtime are communicated with advance notice. However, Zasio cannot guarantee advance notice of Emergency Downtime. Zasio will use best efforts to: (i) limit Hosted Services downtime; (ii) provide Customer with 72 hours' notice of Scheduled Downtime; and (iii) conduct Scheduled Downtime at non-peak hours (based on the time zone where the Hosting Facility data center is located).

4. **Data Center Upgrades**. The Hosting Facility is constantly upgrading its data center facilities, and to benefit from these upgrades, the Hosting Facility may relocate servers within its data centers, make changes to the provision of the services, URLs, and IP addresses, and establish new procedures for the use of the Hosted Services. The Hosting Facility may also make changes to DNS records and zones on Hosting Facility operated or managed DNS servers as deemed necessary for the operation of the shared network infrastructure. Data center upgrades are part of Scheduled Downtime.

5. **Service Level Credits**

5.1 **Credits**. Customer must request a Service Level Credit within 7 days of the Service Level Failure. If Zasio confirms the Service Level Failure, including its duration, Customer may request a Service Level Credit as specified in the table below. Any Service Level Credit will be issued to Customer's account. The credit may be applied to future payments or may be paid out, upon request.

5.2 **Cumulative Dollar Amount**. The maximum total credit for failure to meet the Service Level Guarantee, the Recovery Point Objective, the Recovery Time Objective, or any combination of these, for any calendar month will not exceed 100% of Customer's monthly fee for the affected Hosted Services (calculated from Customer's fee for the then-current Subscription Term). Any Service Level Credit that would be available but for this maximum monthly credit will not be carried forward.

5.3 Termination. In the event there is a Service Level Failure for four consecutive months or for at least five months during any 12 month period, Customer may terminate its subscription for the affected Hosted Services by providing Zasio with written notice within 30 days of the failure. Upon Customer's termination under this SLG Section 5.3, Zasio will refund Customer the amount of any Service Level Credits accumulated to date and the pro rata amount for any unused Subscription Term prepaid by Customer.

Service Level	Target	Minimum	Service Level Credit
Availability of Hosted Services	100%	99.5% (below which constitutes a Service Level Failure)	Zasio will credit 2% of Customer's monthly fee for the affected Hosted Services once a Service Level Failure has occurred. Zasio will credit an additional 2% of Customer's monthly fee for the affected system for every 30 minutes of downtime incurred during that calendar month once a Service Level Failure has occurred.
Customer Data Recovery Point Objective (RPO) – [targeted age of Customer Data that must be restored in case of disaster]	24 hours	48 hours	Zasio will credit 5% of the Customer's monthly fee for the affected Hosted Services for every 24-hour period beyond the minimum RPO.
Recovery Time Objective (RTO) - [Target recovery time for restoring Hosted Services Availability after becoming aware of an unplanned system outage]	2 hours	6 hours	Zasio's target to restore Hosted Services Availability is 2 to 6 hours after becoming aware of any unplanned system outage. Zasio's ability to meet this RTO will depend on the outage's cause and severity. Regardless, Zasio will credit an additional 2% of Customer's monthly Hosted Services fee for every hour of downtime incurred beyond the maximum acceptable outage (which is 6 hours) during a given Service Level Failure.

5.4 Limitations. Customer is not entitled to a Service Level Credit if, at the time of the Service Level Failure, Customer is in material breach of Attachment C or is subject to a suspension or termination of Hosted Services access and use pursuant to Attachment C's terms (including payment obligations to Zasio). Customer also is not entitled to a Service Level Credit if the Service Level Failure would not have occurred but for Customer's breach of Attachment C or misuse of the hosted system. This Service Level Guarantee is contingent on Zasio having full logical access to Customer's configuration. No Service Level Credit will be due if the Service Level Failure would not have accrued but for Customer's restriction of Zasio's logical access to its configuration. The remedies described in this Service Level Guarantee is Customer's exclusive remedy and Zasio's sole liability to Customer for any Service Level Failure, including any related loss of Customer Data hosted in connection with the Hosted Services.

Exhibit 4
Technical and Organizational Measures

Zasio has implemented and will maintain the following Technical and Organizational measures in relation to Zasio's provision of the Hosted Services to Customer under Attachment C. Zasio's Technical and Organizational measures are designed to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks to rights and freedoms of natural persons.

Information security threats are evolving, requiring Zasio to continually improve its Technical and Organizational measures to keep pace with an ever-changing threat landscape. Accordingly, Zasio may update its Technical and Organizational Measures from time to time. Any updates will serve the same purpose and will not materially degrade the Hosted Services' level of security. Zasio's Technical and Organizational Measures, in conjunction with Zasio's security commitments in Attachment C and Exhibit 6, are Zasio's only responsibility with respect to Customer Data.

Capitalized terms used but not defined in the Technical and Organizational Measures are defined in Attachment C.

1. **Security Program.** Zasio shall implement and maintain a comprehensive written Information Security Management System (ISMS) to systematically manage and protect Zasio's business information, as well as the information of Zasio's customers. All security and privacy related policies and procedures are (i) documented, (ii) approved by executive management, (iii) communicated to all personnel, and (iv) reviewed and updated at least annually.

2. **SOC 2, Type 2 Audit Report**. Zasio shall also implement and maintain appropriate administrative, technical, and physical safeguards to protect Personal Data as described in its most recent SOC 2, Type 2 report (or equivalent) received from a qualified third-party auditor. A copy of Zasio's current SOC 2, Type 2 (or equivalent) report is available upon request.

3. **Physical Security.** Zasio's facility and perimeter are monitored and secured using electronic locks and web-enabled video. Visitors must be logged and escorted by Zasio employees. Access to Zasio's facility is electronically restricted outside of normal business hours. Zasio's accounting department, server and network area, and executive offices are protected by additional electronic security designed to prevent unauthorized physical access.

4. **Logical Safeguards.** Zasio utilizes Windows Server 2016 Active Directory to control logical access to its network resources. Unique IDs and strong passwords are enforced by default for all personnel through our network policy configurations. Zasio requires all personnel to use a company-managed, commercial password vault to store all passwords and prevent the unauthorized access or disclosure of passwords. Zasio personnel are also prohibited from reusing old passwords. Passwords for confidential systems must meet Microsoft built-in complexity requirements unless infeasible. Zasio further requires clean desk and clear screen practices through its HR policies.

   Remote access to Zasio's network is allowed only through SSL VPN and granted to personnel on an as-needed basis. Encryption and two-factor authentication are required for all remote access and VPN credentials are maintained through Active Directory.

5. **Data Security.** Zasio's ISMS requirements include (i) conducting an annual risk assessment that is presented to executive management, (ii) conducting tabletop exercises at least annually that involve our information security team's deployment and testing of our Information Security Incident Response Plan, (iii) an internal audit program governed by committee, and (iv) management of Zasio's information security program by committee.

6. **Information Security Team.** Zasio's information security team is comprised of a cross-section of employees from different business units, which includes both in-house legal as well as personnel with appropriate professional certifications, such as the certified information security manager (CISM). The team is responsible for maintaining Zasio's information security controls and works collaboratively with executive

management to monitor information security practices and assist with organizational compliance with information security-related policies and procedures.

7. **Data Center Security**. Zasio systems installed in its facility that are used to process Personal Data are protected by the physical and logical security measures set forth in this Annex. Zasio has contracted with Microsoft Corporation (Azure) as the Hosting Facility which hosts any Hosted Services to which Customer subscribes, including any Customer hosted database. Microsoft's security and compliance controls are described on its website: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all.

8. **Risk Management and Assessments**. Zasio maintains a written risk management policy that defines the methodology for assessing and managing information security, as well as strategic and operational risks.

9. **Access Control Policy**. Zasio maintains a written policy for limiting access to authorized parties with a need to know Zasio information and information processing systems, networks, and facilities.

10. **Vendor Management.** Zasio maintains a vendor management program consistent with industry best practices to ensure Zasio's third-party suppliers comply with contractual and sound security and availability requirements. Zasio ensures that agreements with vendors include appropriate confidentiality and privacy obligations to ensure Zasio can meet its security and privacy obligations.

11. **Software Secure Development Lifecycle**. Zasio maintains a documented software development lifecycle policy to help ensure that industry-standard information security is designed and implemented within the development lifecycle for applications and information systems. This policy incorporates OWASP Top 10 as Zasio's standard for development.

12. **Vulnerability Assessments**. Zasio undergoes penetration testing of Zasio's information systems infrastructure by a qualified third party at least annually. Additionally, Zasio has a qualified third party perform monthly web application scans in connection with our SaaS offerings.

13. **Change Management**. Zasio maintains a change management program to plan, test, communicate, and execute changes affecting our Hosted Services, systems, networks, and applications.

14. **Network Security**. Zasio maintains industry-standard technologies and controls to protect network security, including firewalls, intrusion prevention, monitoring, network segmentation, and VPN and wireless security. Network designs and controls are reviewed at least annually. Zasio utilizes a dedicated firewall/proxy appliance with an enhanced security subscription to help ensure that all communications attempting to cross Zasio's network boundary comply with Zasio's security policy. Several layers of protection are enabled within this firewall for maximum security, including (i) monitoring traffic patterns to detect the presence of potentially sensitive data passing through the firewall; (ii) port blocking so that only required ports are opened and port scans are automatically blocked; (iii) advanced traffic monitoring with cloud-based data analysis and automatic threat response; and (iv) cloud-based DNS-level filtering to detect and block potentially dangerous connections and protect networks and employees from damaging attacks.

15. **Malware Protection**: Zasio utilizes an industry-standard malware protection strategy designed to prevent network virus and other malware outbreaks, as well as prevent network security attacks involving computers attached to Zasio's network.

16. **Data Transfers**: Zasio maintains a Data Management Policy designed to protect customer data coming into Zasio's network. Non-sensitive data transfers are accomplished using a secure FTP (SFTP) site for encrypted file uploads. Zasio also maintains restricted data handling requirements for transferring sensitive data.

17. **Restricting Information Access**. Zasio utilizes the principle of least privilege to manage employee access to information and programs. All personnel are also bound by contractual obligations with Zasio for protecting personal and confidential data.

18. **Background Checks and HR Practices**. Zasio performs pre-employment background checks of all employees, and subsequently on an as-needed basis. Personnel access to software and servers is restricted on an as-needed basis. Zasio also maintains industry-standard on-boarding and off-boarding policies to ensure new hires are properly trained in their roles and security obligations and that access to Zasio information and systems is promptly terminated upon any personnel departure. All employees are additionally bound by Zasio's Business Ethics and Code of Conduct.

19. **Business Continuity and Disaster Recovery.** Zasio maintains a formal BC/DR plan to help ensure that Zasio's systems and services remain resilient in the event of any extended service outages. Zasio conducts a disaster recovery test utilizing this plan (including testing of the backup restoration process) at least annually.

20. **Data Backup and Recovery**. Zasio maintains a formal backup and recovery plan to help ensure that all information is regularly backed up and to establish recovery time and recovery point objectives in the event of any unplanned system outage.

    - **Hosting Facility Backups**. Each database and dedicated server in Zasio's Hosting Facility undergoes a (i) daily, point-in-time-restore (hot) backup, which is retained for two weeks; and (ii) monthly backup, which is retained for three months. Zasio's Hosting Facility tests backup and recovery systems regularly, and in accordance with industry certification standards and best practices.

    - **Internal Backups**. Zasio's major systems (including Active Directory catalogs, email servers, document stores, production databases, and application servers running critical business functions) are fully backed up on a weekly basis, with backup media rotated offsite to a secure location. Incremental backups of active document repositories are captured every two hours.

    Zasio tests both internal and hosted backup and recovery systems at least annually.

21. **Information Security Incident Response Planning**. Zasio maintains a formal information security incident response plan which must be activated in the event of any Information Security Incident or related event. Zasio maintains a record of any information security breach with a breach description, the time period, consequences of the breach, identity of the reporter, and the procedure for recovering data.

22. **Data Segregation**. For Hosted Services customers, Zasio maintains separate hosted databases for each customer, with permissions that only allow user access for the one database to which that customer is associated. Zasio also maintains separate internal production and test database servers to protect against unauthorized access to Personal Data.

23. **Encryption of Customer Data**. Zasio utilizes strong encryption of Personal Data both in transit and at rest. Zasio also requires the encryption of all mobile computing devices used to transmit or store Personal Data.

24. **Security Training**. Zasio conducts security awareness training for all personnel upon hire and at least annually, and provides security awareness updates at least quarterly.

25. **Asset Management**. Zasio maintains a formal IT asset management policy, which utilizes real-time accounting of all Zasio IT assets as well as industry-standard secure disposition of all IT assets at the end of their lifespan with the company.

26. **Customer Data Deletion**. Zasio maintains formal customer data deletion policies and procedures to help ensure that all Customer Data within Zasio's possession, custody, or control is timely deleted in accordance with Zasio's contractual and legal requirements.

27. **Log Data**. Zasio maintains a Security Information and Event management (SIEM) and anomaly detection program in respect of the Hosted Services. Associated log data is retained for up to 1 year for purposes of conducting forensic analysis of security incidents.

Exhibit 5

Zasio Records and Information Management (RIM) Professional Services Supplemental Terms

These Zasio Records and Information Management (RIM) Professional Services Supplemental Terms (these "RIM **Professional Services Terms**") form part of the Parties' Master Agreement and Attachment C to which it is attached. These RIM Professional Services Terms set forth the supplemental terms applicable to Zasio's provision of Professional Services (defined below) to Customer pursuant to a mutually executed SOW.

Capitalized terms not defined in these RIM Professional Services Terms are defined in the Attachment C or the Master Agreement. In case of conflict the more specific of these RIM Professional Services Terms will prevail over the more general terms of the Attachment C, but only to the extent of any conflict concerning RIM Professional Services.

1. PROVISION OF RIM PROFESSIONAL SERVICES

1.1 Description of Services. Zasio will perform the records and information management professional services (the "RIM **Professional Services**") specified in a statement of work (each an "**SOW**") entered into under the Attachment C. The Parties' SOW No. 1is attached as **Annex A** and forms part of this Exhibit 5. For any subsequent SOWs, the Parties may utilize the form of Annex A. Each mutually executed SOW will form part of Attachment C as long as it specifically references the Attachment C.

1.2 Deliverables under this Attachment C. RIM Professional Services may include the delivery of tangible work product (such as written reports, data maps, retention schedules, research, assessments, policies, procedures, guidelines, plans, training materials, and other working papers) in hard or electronic form ("**Deliverables**") for Customer's Internal Business Use. All Deliverables will be expressly identified in the applicable SOW.

1.3 RIM Professional Services Personnel. "**Consultant**" means any Zasio employee or other personnel who provides RIM Professional Services to Customer. Zasio Consultants will have the requisite knowledge, skill, and experience to successfully perform RIM Professional Services. Customer shall promptly notify Zasio of any concerns regarding a Consultant. The Parties shall then mutually determine the best way to resolve these concerns, which may include the Consultant's reassignment. Zasio otherwise has sole discretion to select the Consultants it uses to provide RIM Professional Services to Customer and reserves the right to replace any Consultant at any time with a Consultant having equivalent skills.

1.4 Change Procedure. "**Change**" for these RIM Professional Services Terms means any material change to the scope or parameters of RIM Professional Services requested by either Party. The Party requesting a Change must notify in writing the other Party's designated individual detailing the Change and the reasons for it. The Parties shall negotiate in good faith the Change and any revised fees. Prior to implementing any Change, the Parties shall execute a change order that will detail the Change along with any modified terms and associated fees, and that change order will form part of Attachment C. Upon the Parties' written acknowledgment at the time, the Parties may amend the timetable to any SOW without needing to complete a formal change order.

1.5 SOW Conflicts. In the event an SOW's terms conflict with the terms of these RIM Professional Services Terms or Attachment C, the SOW will govern to the extent applicable to the RIM Professional Services.

1.6 Cooperation. To help ensure that Zasio is able to provide timely and successful RIM Professional Services, Customer agrees to:

- **a.** Timely provide Zasio with all Customer Data reasonably necessary for Zasio to provide RIM Professional Services;

b. timely review and provide input on draft and final Deliverables in accordance with any timeframes established in an SOW;

c. making available at least one agreed-upon representative to Zasio who possesses the relevant knowledge and experience to act as a project manager under any SOW.

Zasio's obligations will be conditioned upon Customer's material compliance with this Subsection 1.6 as may be reasonably necessary to perform the RIM Professional Services. Also, any Customer Change that materially impacts Zasio's schedule, as well as any other Customer-caused delays to the provision of Services, will cause an SOW's timetables to be extended by the length of the Customer-caused delay.

2. PAYMENT

2.1 Compensation. All fees for RIM Professional Services are stated in and must be paid in U.S. dollars, unless the Parties expressly agree otherwise in writing. Zasio's billing rates and frequency (such as monthly, per milestone, or lump sum) for RIM Professional Services will be established in the applicable SOW. Customer must pay all undisputed invoices within 30 days of receipt. If Customer fails to pay any undisputed fees within this 30-day timeframe, Zasio may terminate the applicable SOW, these RIM Professional Services Terms, or Attachment C pursuant to Section 8.3.a. Unless the Parties expressly agree otherwise in an SOW, fees for RIM Professional Services will include all materials.

2.2 Travel and Expenses. Costs for travel and related out-of-pocket expenses will be in addition to fees for RIM Professional Services. Zasio will bill for any travel and related out-of-pocket expenses at actual cost in accordance with Customer's reasonable travel policies. Zasio will comply with Customer's then current travel and expense policy when this policy is provided in advance. Any airline travel will be in economy or like class to be eligible for reimbursement.

3. INTELLECTUAL PROPERTY RIGHTS AND USE RESTRICTIONS

3.1 Ownership. Subject to the provisions of this Section 3, Customer will own all Deliverables produced under these RIM Professional Services Terms. However, Zasio shall continue to own and have an unrestricted right to use for other purposes Zasio's proprietary information and intellectual property contained in any Deliverable, which includes all:

a. formats related to the Deliverables;

b. processes for the Deliverable's development;

c. legal annotations or summaries created by Zasio; and

d. Zasio's proprietary products or processes, regardless of whether developed before or after the Effective Date.

(collectively, "**Zasio Property**").

To the extent any Zasio Property is contained in a Deliverable, Customer shall have a perpetual, non-exclusive license to use, copy, and distribute that Zasio Property and create derivative works from it for Customer's Internal Business Use.

3.2 Archival Copies. Zasio may retain archival copies of any Deliverable subject to Zasio's confidentiality obligations related to Confidential Information (in accordance with Section 3 of the Master Agreement) for

Zasio's Internal Business Use, and nothing in this Attachment C will prevent Zasio from continuing to use Zasio Property.

4. LIMITED WARRANTY

4.1 RIM Professional Services Warranty. Zasio warrants that it will perform the RIM Professional Services in a professional and workman-like manner in accordance with prevailing records and information management industry standards. Upon delivery, the Deliverables will materially conform with the applicable specifications as set forth in the applicable SOW.

4.2 Notification. Customer must notify Zasio in writing within 90 days of Zasio's provision of RIM Professional Services of any alleged breach of Zasio's RIM Professional Services Warranty and provide Zasio with all relevant information reasonably necessary for Zasio to correct the alleged defect.

4.3 Remedy. Upon receiving Customer's timely notice of any alleged RIM Professional Services Warranty breach, and if Zasio validates the existence of the alleged breach, Zasio will reperform the applicable RIM Professional Services or Deliverables within a commercially reasonable time. If Zasio's reperformance does not remedy the defect, Zasio will refund any fees for the defective RIM Professional Services actually paid by Customer. The remedies in this RIM Professional Terms Section 4.3 are Customer's sole and exclusive remedy, and Zasio's exclusive remedy, for any breach of Zasio's *Consulting Services Warranty*.

4.4 Warranty Disclaimer. EXCEPT FOR THE EXPRESS WARRANTY IN THIS RIM PROFESSIONAL SERVICES TERMS SECTION 4, ZASIO EXPRESSLY DISCLAIMS ALL WARRANTIES FOR RIM PROFESSIONAL SERVICES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ALL RIM PROFESSIONAL SERVICES, INCLUDING ALL DELIVERABLES, ARE OTHERWISE PROVIDED "AS IS." CUSTOMER IS RESPONSIBLE FOR REVIEWING THE DELIVERABLES TO ENSURE THEIR ACCURACY AND COMPLETENESS AS WELL AS FOR THE RESULTS OBTAINED FROM CUSTOMER'S USE OF THE DELIVERABLES.

4.5 Liability Limitations for RIM Professional Services. The liability limitations, exclusions, and exceptions set forth in Section 5 of the Master Agreement apply to the Parties in connection with Zasio's provision of RIM Professional Services. However, for any claim concerning RIM Professional Services provided under the Attachment C, the maximum allowable damages will not exceed the total fees paid or payable for the applicable RIM Professional Services under the relevant SOW.

5. DEFENSE AND INDEMNIFICATION

The Parties' defense and indemnification obligations under Section 11 of Attachment C will apply in connection with the provision of RIM Professional Services, except that when applied to these RIM Professional Terms, RIM Professional Services will replace the term Hosted Services and SOW will replace the term Order Form.

6. Term and Termination

6.1 Term. The Parties may continue to enter into SOWs for RIM Professional Services under these RIM Professional Services Terms and the Attachment C until the Attachment C is expressly terminated.

6.2 Termination at Will. Customer may terminate these RIM Professional Services Terms or any SOW under these RIM Professional Services Terms without cause upon 30 days' written notice to Zasio.

6.3 Rights Upon Termination. Upon any termination of the Attachment C, these RIM Professional Services Terms, or any SOW for RIM Professional Services, Customer shall: (1) pay all undisputed costs and fees for RIM Professional Services incurred prior to termination; and (2) have no right to use the Deliverables or the information provided by Zasio as part of RIM Professional Services unless Customer has paid all fees and costs related to the Deliverables. Upon termination, each Party shall promptly comply with Section 3.4 of the Master Agreement regarding return or destruction of Confidential Information.

[End of RIM Professional Services Terms]

Annex A to Attachment C (RIM Professional Services Terms)

STATEMENT OF WORK # 1

FOR

RIM PROFESSIONAL SERVICES

This Statement of Work for RIM Professional Services ("**SOW**"), effective as of the Master Agreement Effective Date ("**SOW Effective Date**"), is between Zasio Enterprises, Inc. ("**Zasio**") and the City of San Diego, a California municipal corporation, ("**Customer**") pursuant to the Parties' Master Agreement, and specifically, Exhibit C (the "**Master Agreement**"). Capitalized terms not defined in this SOW are defined in the Master Agreement and Exhibit C.

1. **Project Summary**. Zasio will assist Customer with refreshing Customer's Records Retention Schedule (RRS). Specific items include conducting research to identify relevant recordkeeping requirements within the in-scope jurisdictions, mapping identified requirements with particularity to the RRS, and providing recommendations to account for jurisdictional requirements as necessary. Zasio's approach and methodology to accomplish these tasks are explained in greater detail below.

2. **Scope of Work**. Zasio will perform the following RIM Professional Services under this SOW:

   Task 1: Recordkeeping Research

   Zasio will conduct research for laws and regulations applicable to the records identified in Customer's RRS. Zasio will conduct research for the following jurisdictions:

   1. United States (Federal)
   2. California
   3. San Diego Municipal Code

   Zasio will conduct research in a logical and orderly manner, from the general to the specific, in accordance with the following methodology:

   - **Generic records search queries** – Initially execute search queries that are broadly formulated. The resulting list of potentially relevant requirements is then manually scanned and flagged for further analysis.

   - **Searches by subject areas of Customer's business** – Targeted searches are conducted for the specific areas of Customer's business as reflected in its RRS using key words and types of records identified from the RRS. Additionally, these terms are used to refine the results from the generic records search.

   Research Scope

   The research scope includes requirements for retention, data privacy (limitations on keeping personal data), records handling (e.g., format, location, and destruction) requirements and select statutes of limitation. Each research scope is described in greater detail below.

   Retention Laws and Regulations: These include laws and regulations where a period of retention is expressly stated but excludes those where no specific period of retention is prescribed.

   Privacy: Covers privacy laws regulating the retention of records that are or contain information classified as "personal data," "personally identifiable information," or other similar variations (collectively "personal data")

within the in-scope jurisdictions. Applicable privacy laws generally limit the retention of records that contain personal data. To ensure consistency in application, Zasio will identify the record types potentially impacted by or which contain the regulated personal data. Zasio will submit this list to Customer for confirmation and approval.

Handling Requirements: These requirements consist of:

- Destruction: Mandates the manner of destruction of records after the legally specified retention period expires.
- Records Location and Movement: These provisions may require records be held at the "head office," or "principal place of business," in the jurisdiction in question. They also restrict the movement of records (e.g., cross-border transfers).
- Records Media / Format: Requires or restricts the retention of records to a format type (e.g., physical or electronic) or specifies a media for recordkeeping (e.g., microfiche).

Statutes of Limitations: When a jurisdiction has a law requiring the retention of records in a record type, Zasio will rely on it to make its retention recommendations. Statutes of limitations (including statutes of prescription) (collectively, "SoLs"), however, generally do not mandate the retention of records. Instead, SoLs provide additional grounds to consider when setting an appropriate retention period. Nonetheless, Zasio will identify any tendency among organizations to rely on SoLs as a retention driver ("Retention Driver SoLs"). Also, given the large number of SoLs, Zasio's research focus is limited to the most requested SoLs. This includes SoLs related to contracts, personal injury, worker's compensation, wage claims, design/construction, real estate ownership, and tax. To ensure consistency in application, Zasio will identify the record types potentially impacted by or which contain the regulated SoLs. Zasio will submit this list to Customer for confirmation and approval.

Task 2 – Research Mapping/Application & Recommendations

For the in-scope jurisdictions, Zasio will review the RRS baseline retention periods and recommend necessary adjustments to increase retention periods based on determinative citations serving as "retention drivers" or decreases to retention periods to meet maximum retention requirements that compel destruction of records.

Zasio will note compelled privacy requirements separately for Customer's consideration. Where these requirements apply to a record within a functional bucket containing numerous records or affect a mixed use (i.e., the purpose of the record has multiple functions within the organization and introduction of a short retention period may affect its operational value) Zasio will identify these requirements separately for consideration next to the record series to which they apply.

Zasio will also map relevant SoLs to the applicable record series. However, because these are not retention mandates, they are generally not relied on for retention recommendations unless Zasio's experience with the in-scope jurisdiction indicates a tendency, in practice, to so rely. In those situations, Zasio will identify the applicable SoLs in the retention driver field.

Zasio will analyze and identify the citation establishing the longest required retention period for each record class. Zasio's methodology is to review all linked citations to determine the longest and most broadly applicable requirement for each record class. Zasio will use the longest recordkeeping citations to recommend further reductions to retention periods where feasible based on legal requirements and common industry recordkeeping practices. Longest recordkeeping citations are provided as part of the final deliverable.

Lastly, all remaining handling requirements, i.e., those related to location, movement, media, format, and destruction, will be mapped to the applicable record series.

Customer Review and Approve

Zasio will work with Customer to review, explain, answer questions, and approve or reject all recommended adjustments to Deliverables.

Finalize and Deliver RRS

Zasio will then finalize the Deliverables to reflect adopted recommendations and necessary adjustments. Zasio will deliver the Deliverables in spreadsheet, MS Word, PDF, or another mutually agreeable format.

3. **Deliverables.** Zasio will provide the following Deliverables to Customer:

   - Recommendations based on Recordkeeping Research
   - Finalized RRS and linked research delivered via the Versatile 2023 **On-Premise or** SaaS application, Excel, or another agreeable format.

4. **Timetable.**

The noted dates are estimates only and the final timetable is to be determined following consultation between Customer and Zasio to formalize. The final formalized timetable will be subject to other Zasio client commitments that arise during the interim. The project shall commence no earlier than April 1, 2024.

Task/Deliverable	Estimated Time	Responsible Party
Project Kickoff	Week 1	Zasio/Customer
Task 1: Recordkeeping Research	Weeks 2-8	Zasio
Task 2: Research Mapping/Application & Recommendations	Weeks 6-12	Zasio
Customer Review and Approve	Weeks 13-14	Customer
Finalize and Deliver RRS	Weeks 15-16	Zasio

*Tasks with overlapping weeks may run concurrently.

5. **Nature of Services.** The Services under this SOW, including all Deliverables, are provided with Customer's understanding that Zasio is not a law firm and does not provide legal advice or services. Zasio provides all Services from a RIM perspective and based on experience with other customers. All decisions related to records and information management, including recordkeeping, records retention, and privacy, should be reviewed and approved by Customer's legal counsel.

6. **Fees.** The following fees for the work under this SOW do not include any travel expenses:

Task 1: Recordkeeping Research $6,000.00
Task 2: Research Mapping/Application, & Recommendations $5,000.00
Task 3: Finalize and Deliver RRS $5,000.00

Grand Total $16,000.00

All prices are in U.S. dollars. Services are invoiced at the conclusion of each task in this SOW. Sales tax is not included in the above prices but will be calculated and reflected in the applicable invoice for these Services.

Travel is not anticipated for this project. However, if travel is required and approved, travel expenses (e.g., airline, hotel, food, car, etc.) will be billed at actual cost with no markup and copies of travel expenses will be provided upon request. Zasio will adhere to Customer's reasonable travel policies.

7. **Term.** This SOW's term shall begin on the SOW Effective Date and shall continue until the Services are completed or until the SOW is otherwise terminated pursuant to the Master Agreement.

The Parties have caused this SOW to be executed by their duly authorized representatives to be effective as of the SOW Effective Date.

[***The Parties' Signatures to the Master Agreement also constitute the Parties' signatures to this SOW No. 1***]

Exhibit 6

City of San Diego Technical and Security Administrative Regulations

Attached to the following pages:

1. Administrative Regulation 90.63, Issue 2, Effective May 5, 2017.
2. Administrative Regulation 90.64, Issue 2, Effective May 5, 2017.
3. Administrative Regulation 90.68, Issue 1, Effective April 14, 2021.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
	90.63	2	1 of 12
INFORMATION SECURITY POLICY	Effective Date May 5, 2017		

1. PURPOSE

1.1. To ensure *City Information* is accurate, relevant, properly protected, and handled consistent with City policies and *Standards*.

1.2. To establish *Information Security Policies* and procedures for protection of *City Information* and the use of City *Computer Equipment*, Network Services, and *Electronic Mail* (*Email*) and non-City or personal *Computer Equipment* that may be used to access City *Computer Equipment*, *Computer Systems* or *Network Services* by any person or affiliate that is subject to this Administrative Regulation.

1.3. To establish a procedure for approving and notifying employees, and other individuals and entities subject to this Administrative Regulation, about *Information Security Standards and Guidelines* that will provide specific guidance and criteria in securing and using City *Computer Equipment*, *Network Services*, and *Email*.

1.4. To establish the basis for an Identity Theft Prevention Program, to ensure the security and safety of both employee and citizen/customer personal information.

2. SCOPE

2.1. This regulation applies to all City employees, contractors, volunteers, and other affiliates, sometimes collectively referred to as "Individuals," using some or all of the City of San Diego's *Computer Systems*, Computer Equipment, *Network Services* or Email system.

2.2. This regulation applies to the use of City *Computer Equipment* or *Network Services* and to non-City or personal computer equipment that may be used to access City *Computer Systems* or *Network Services* by any Individual subject to this Administrative Regulation.

3. DEFINITIONS

3.1. *Breach* - Means unauthorized access to the City's Computer Equipment, *Computer Systems*, Email, or *Network Services* was, or is reasonably believed to have been, acquired by an unauthorized person.

(Supersedes Administrative Regulation 90.63, Issue 1, effective June 30, 2011)

Authorized

(*Signature on File*)

CHIEF OPERATING OFFICER

3.2. *City Information* - Includes information relating to the conduct of the public's business which is prepared, owned, used or retained by any City department or Individual regardless of physical form or characteristics.

3.3. *Computer Equipment* - Includes computer hardware and peripherals, including monitor, mouse, keyboard, and printers, tablets, portable or laptop computers, smart phones and similar communication equipment owned, operated or maintained by the City or an information technology (IT) service provider under contract with the City.

3.4. *Computer Systems* - Includes a network system, interconnected *computer equipment* (e.g., servers and storage devices), software package, or other IT resources.

3.5. *Email (Electronic Mail)* - A method of composing, storing, sending, and receiving (electronic transfer of information) electronic messages, memoranda, and attached documents from a sender to one or more recipients via a telecommunications network.

3.6. *Guidelines* - Recommended actions and/or industry best practices that should be used regarding security practices for ensuring compliance with policies and *standards*.

3.7. *Information Security* - An attribute of information systems which includes specific policy-based mechanisms, practices, procedures, and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.

3.8. *Information Security Standards and Guidelines* - Means the *standards* and *guidelines* developed by the Department of IT and approved by the appropriate IT governance body which govern operation of City *Computer Systems*, *Computer Equipment*, *Email*, and *Network Services*.

3.9. *Information Security Policies* - Organizational rules and practices that regulate how an organization manages, protects, and uses its information system assets and data.

3.10. *Internet* - A publicly accessible network connecting *Computer Systems* throughout the world using the standard *Internet* Protocol (IP). In addition to providing capability for *Email*, other *Internet* applications include, but are not limited to, news groups, data processing & storage services, data transfer services, *Email*, cloud services, and the world-wide web ("WWW" or "Web").

3.11. *Network Services* - Communication networks, including the underlying infrastructure of routers, switches, wireless access points, and communications media for hard-wired or wireless transmission of data across the network. Local Area Networks (LANs), Wide Area Networks (WANs), the *Internet*, and wireless networks are examples of *Network Services*.

3.12. *Standards* - Indicates how and what kind of software, hardware, databases, and business practices should be implemented, used, and maintained to meet security and operational objectives.

3.13. *System Managers or System Administrators* - Individuals who support the operations and integrity of City *Computer Systems* and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. By the nature of their duties, they have administrative-level access to *Computer Systems*, including operating systems, applications, databases, software utilities, and computer hardware, not accessible by standard *Users*.

3.14. *User* - Any individual who has been granted privileges and access to City *Computer Equipment*, *Network Services*, applications, resources, or information. *User* is also any person who is identified in Sections 2.1. and 2.2. above.

3.15. *User ID or User Account* - The unique account identifier that is assigned to a *User* of the City's *Computer Equipment*, *Computer Systems*, and *Network Services*.

4. POLICY

4.1. General

4.1.1. Guidance, direction, and authority for *Information Security* activities are centralized for the City under the Department of Information Technology ("Dept. of IT"), Chief *Information Security* Officer (CISO).

a. The Dept. of IT will provide direction and expertise to ensure the City's information is protected. This responsibility includes consideration of the confidentiality, integrity and availability of both information and *Computer Systems* that manage information. The Dept. of IT will act as a liaison for all *Information Security* matters with all City departments and IT service providers, and must be the focal point for all *Information Security* activities throughout the City. The Dept. of IT will participate in vendor product evaluations and in-house system development projects, assist with implementing security controls, investigate *Information Security Breaches* and perform other activities which are necessary to assure a secure information handling environment.

b. The Dept. of IT has the authority to provide exceptions to specific provisions of this policy based upon unique business requirements and other considerations. Departments will promptly notify the Dept. of IT in the event an exception is being requested for the security requirements of their respective *Computer Systems*. All exception requests and resulting actions must be fully documented and will be retained by the Dept. of IT.

4.1.2. All computer files developed, created or enhanced within the scope and course of City employment, or a City third-party contractual relationship, are the property of the City of San Diego, regardless of their physical location or the form in which they are maintained. These include, but are not limited to, computer data files, documents, databases, spreadsheets, calendar entries, appointments, tasks, and notes which reside on any City *Computer Systems* or *Computer Equipment*, or the *computer equipment* of a contractor performing work for or on behalf of the City.

a. The City reserves the right to access and disclose as required or permitted by law, and as defined in the approved *Information Security Standards and Guidelines*, all messages and other electronic data sent over its *Email* systems or stored in computer files on City *Computer Equipment*. City-related computer files stored on non-City or personal computers must be provided upon the City's request in City standard formats.

b. It is the responsibility of the Department Head or designee to ensure access to City *Computer Systems* is terminated and all computer files are properly handled by the City when an employee leaves City employment, pursuant to applicable City regulations, policies, and procedures.

c. All inventions, improvements, developments, or other works and any related copyrights, trademarks, patents or other intellectual property rights which are in any way related to City business or activities and which are created, developed, enhanced, or are derived, by one or more City employees during the employee's employment and compensated working hours, or using City *Computer Equipment*, or otherwise developed within the scope of an employee's employment, are the exclusive intellectual property rights of the City of San Diego and the City shall own all rights in such intellectual property, including any applicable copyright, patent, trademark, or other intellectual property rights.

4.1.3. Access to information available through the City's *Network Services* or from the City's *Computer Systems* is controlled by Dept. of IT approved access control criteria and *Information Security Standards and Guidelines*, which are to be maintained and reviewed at least annually, including updates, as necessary.

4.1.4. Authorized access to City *Computer Systems* and *Network Services* shall be at the minimum level required for the Individual to perform and complete their assigned duties, and not at a level that allows access to information beyond the scope of that Individual's assigned duties.

4.1.5. Each *Computer System* or *Network Services User ID* must uniquely identify only one *User*. Generic, shared, or group *User IDs* are not permitted. Any unique *User ID* shall not be duplicated across multiple *user* authentication directories,

so that there is always only one source *User* directory for authenticating any *User ID* for access to City *Computer Systems* or *Network Services*. Network security groups may be used to combine *Users* access rights. Approved group *Email* accounts may be shared by multiple *Users* who each have unique *User IDs*.

a. Any Department that requires Individuals to share a single *Computer System*, such as a desktop PC used for customer service, must ensure compliance with the shared-use workstation requirements of the *Information Security Standards and Guidelines.*

4.1.6. The initial login password issued to a *User* must be valid only for that *User*'s first online session. At the time of initial login, the system must force the *User* to create another password before any other work can be done on the system. Passwords must meet the current criteria set in the *Information Security Standards and Guidelines.*

4.1.7. *Network Services* are an essential component of the City's information resources. No device may be connected to the City's *Computer Systems*, data network or voice network unless it has been specifically approved by the Department of Information Technology (IT) pursuant to *Information Security Standards and Guidelines* adopted in accordance with this policy. This section excludes portable data storage devices/media, such as USB drives, being connected to an existing City computer, as long as proper security measures are taken with those devices to prevent and avoid infection by malicious software (i.e., virus or Trojan).

4.1.8. All servers, network equipment or telecommunications equipment used for the production support of City business operations must utilize uninterruptible power supply (UPS) and surge protection. Devices deemed critical to City business operations should be on dual power grids or on emergency power generators to protect against power outages.

4.1.9. Portable storage devices should only be used for temporary storage of data. Any City data or records created on portable storage devices, such as CDs or USB drives, are to be treated according to Section 4.1.2. above. The content should be made accessible in a standard format and should comply with the *Information Security Standards and Guidelines*. City records stored on portable storage devices must be retained in accordance with applicable laws, rules, regulations, and policies pertaining to the management and retention of City records.

4.1.10. Misrepresenting, obscuring, suppressing, or replacing a *User's* identity on an electronic communications system is forbidden. The *User* name, *Electronic Mail*

address, and related information used for login/access and included with messages or online postings must reflect the actual originator of the messages or postings.

4.1.11. *Users* shall not download or store software from the *Internet* on City *Computer Equipment* which has not been properly licensed to the City or in which the City does not have a legal right to possess or use. *Users* shall not install unauthorized or unlicensed software programs on City *Computer Equipment*. Any authorization must be obtained in advance from the Department of IT.

4.1.12. An *Information Security* Committee or its successor, as defined and chartered through the City's IT governance structure, will meet periodically to review the current status of the City's *Information Security*, review and monitor security incidents within the City, approve and periodically review *Information Security* projects, and provide semi-annual reports related to these activities to the Dept. of IT.

a. The *Information Security* Committee will review this policy and the related *Information Security Standards and Guidelines* annually during the first quarter of each fiscal year, making recommendations for any updates to the Dept. of IT. The Dept. of IT will forward any recommended updates to the City executive management team for approval.

4.2. Departmental Management Policy

4.2.1. Department Directors are ultimately responsible for departmental compliance with the provisions of this policy and other *information security* and acceptable use policies.

4.2.2. Senior management will lead by example by ensuring *Information Security* is given a high priority in all current and future business activities and initiatives.

4.2.3. Management must provide all *Users* within their department with sufficient training to allow them to understand their personal responsibilities to properly protect information resources, including tracking of the dates and names of employees trained. *Information Security* training materials will be created, maintained, and made available by the Dept. of IT. Such training should occur within the first 90 days of employment, and then refresher training should occur annually for all employees.

4.2.4. Management must allocate sufficient on-the-job time for *Users* to acquaint themselves with *Information Security Policies*, separately from the formal training required in Section 5.3 above, including the *Information Security Standards and Guidelines* with related procedures on prohibited activities and

appropriate ways to report security threats. Management must notify *Users* of specific actions that constitute security violations and that such violations will be logged.

4.2.5. Each department will designate an *Information Security* Liaison (ISL) to be the primary point of contact responsible for department compliance with the City's *Information Security Policies* and coordination with the Dept. of IT. The *Information Security* Liaison should be a senior IT staff member or unclassified manager. The City's Chief *Information Security* Officer will manage the ISL program and provide information and training pertinent to the position to assist in protecting City IT assets.

4.2.6. Each department will review their own security practices at least annually for conformance with this policy and compliance with the *Information Security Standards and Guidelines*.

4.2.7. All department and City *Computer Systems* privileges must be promptly terminated at the time a *User* leaves City employment or ceases to provide services to or receive services from the department or the City. Such termination of access to City *Computer Systems* includes revocation of the assigned *User ID* and must occur as soon as possible and, in any case, no more than three (3) business days, after access is no longer required. All files held in the *User's* home directory, as applicable, will be held for 90 days for their supervisor or designee to review and will then be deleted. All City records shall be retained in accordance with the department's approved Records Disposition Schedule or the Citywide General Records Disposition Schedule

4.2.8. Records reflecting the *Computer Systems* on which *Users* have accounts must be kept up-to-date and reviewed periodically, at least annually, by the respective Department Head or designee, so *Computer Systems* access privileges may be expeditiously revoked on short notice, if the need arises.

4.2.9. To provide evidence for investigation, prosecution or disciplinary actions, relevant *Computer Systems* information should be immediately captured and preserved whenever it is suspected that a computer *Breach*, crime or abuse has taken place. The relevant information must be securely stored offline until such time as legal counsel determines the City will no longer need the information. The information to be immediately collected shall include the current system status and backup copies of all potentially involved files. The *Information Security* Liaison or *User* who discovers the suspected *Breach*, crime or abuse should report such to the Dept. of IT, Chief *Information Security* Officer who will take action to preserve the relevant information.

4.2.10. To ensure a quick, effective, and orderly response to *information security* incidents, the *Information Security* Committee will identify a "Cyber Security Incident Response Team" (CSIRT) comprised of IT staff to handle the reporting of and response to *information security* incidents. The reporting of incidents will be done according to the *Information Security Standards and Guidelines*

.

4.2.11. All known vulnerabilities of the City's *Computer Systems*, in addition to suspected or known violations, must be communicated in an expeditious and confidential manner to the Dept. of IT, the Chief *Information Security* Officer, the IT Service Provider, and any others designated by the Dept. of IT.

4.2.12. Except as specifically provided for in this policy, other *Information Security Policies* and procedures or otherwise provided by law, reporting *information security* violations, problems or vulnerabilities to any person outside the City, except to an appropriate government or law enforcement agency, without the prior written approval of the Dept. of IT, is strictly prohibited

4.2.13. Criticality levels will be assigned to each business application to reflect the potential impacts resulting from a *Breach*, data corruption or denial of service. No less than once every two years, the Dept. of IT will conduct a rating survey to inventory and assign criticality levels to City applications. Each Department Director or their designee will assign criticality levels and data elements based on criteria established by the *Information Security* Committee. The Dept. of IT will maintain a master list of all inventoried applications and assigned ratings.

4.3. *User* Policy

4.3.1. *Users* must be responsible in their use of City *Computer Equipment*, and *Network Services*. Any action that may cause interference with City *Computer Systems* exposes the City's *Computer Systems* to risk or adversely impacts the work of others in using these *Computer Systems* is prohibited.

4.3.2. Employees may be disciplined in accordance with standard City procedures for improperly using or knowingly allowing the improper use of the City's *Computer*

4.3.3. *Equipment, Network Services* or *Email* system as stated in this regulation. Abuse of the City's *Computer Systems* may result in disciplinary action, up to and including termination and criminal prosecution if deemed appropriate.

4.3.4. Employees should cooperate fully with all investigations, regarding the abuse of the City's *Network Services, Computer Equipment, Computer Systems*, and the *Internet*.

4.3.5. Every end *User* must have a single unique *User ID* and a personal password which must be kept confidential and not shared with anyone else. This *User ID* and

password will be required for access to all multi-*user Computer Equipment* and *Network Services*. *User* passwords must comply with the *Information Security Standards and Guidelines*.

4.3.6. *Users* accessing City *Computer Systems* are prohibited from gaining unauthorized access to any other non-City *computer systems* or in any way damaging, altering or disrupting the operations of those systems. *Users* are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

4.3.7. Employees who use City *Computer Systems*, *Computer Equipment*, *Network Services*, or the City's *Email* shall sign an *Information Security* Policy Acknowledgement Form which states that the employee agrees to comply with the terms of this Administrative Regulation.

4.4. System Manager/Administrator Policy

4.4.1. Every multi-*user* system must include sufficient automated tools to assist *System Managers* in verifying the security status of the *Computer Equipment* and *Computer Systems*. These tools must include mechanisms for automated notifications to be sent to *System Managers* and for the correction of security problems.

4.4.2. Whenever a City *Computer System* has been *Breached* by an unauthorized party, or there is a reasonable suspicion of a *Breach* or other system compromise, *System Managers* must immediately change the password on the involved system and any other systems at risk from the *Breach*ed account. Under either of these circumstances, all recent changes to *User* and system privileges must be reviewed for unauthorized modifications.

4.4.3. Production application systems which access financial or sensitive information must generate logs that show every addition, modification, and deletion to such information.

4.4.4. Mechanisms used to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software or the logs themselves

4.4.5. All *Computer Systems* and application logs must be maintained in an environment where they cannot readily be viewed by unauthorized persons. By definition, a person is unauthorized if he or she is not a member of the authorized network security group(s) which allow access to such logs.

4.4.6. Logs of computer security related events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures. Logs containing computer security related events must be retained in accordance with the applicable department's Records Disposition Schedules or the Citywide General Records Disposition Schedule. During this period, the logs must be secured so that they cannot be modified, and so that they can be read only by authorized persons. These logs are important for error correction, forensic auditing, security *Breach* recovery, and related efforts.

4.4.7. To allow proper remedial action, *System Managers* must, on a daily basis, review records reflecting security relevant events on multi-*user* machines/systems.

4.4.8. When a person who is authorized as a System Manager or System Administrator ceases to perform those functions, then such person's access to City *Computer Systems*, *Computer Equipment*, *Network Services*, and applications must be immediately revoked and system-level passwords to which he or she had access must be changed as soon as possible and, in any case, no more than twenty-four (24) hours after such System Manager or System Administrator ceases to perform those functions. In addition, such person's physical access to City *Computer Systems*, *Computer Equipment*, and *Network Services* must be restricted or revoked immediately, as appropriate.

5. RESPONSIBILITY

5.1. Mayor

5.1.1. The Mayor will establish regulations and procedures regarding the security and safeguarding of City data, *Computer Equipment*, *Computer Systems*, and *Network Services*.

5.2. Chief Information Officer

5.2.1. The Chief Information Officer has the responsibility to provide *Guidelines*, strategic direction, oversight, and coordination of citywide *Computer Systems*.

5.3. Chief *Information Security* Officer

5.3.1. The Chief *Information Security* Officer or designee will direct and manage the planning and supervision of all *Information Security* services for the City, including those provided by vendors/providers.

5.4. Strategic Technology Advisory Committee (STAC)

5.4.1. The Strategic Technology Advisory Committee (STAC) or other IT governing

body as assigned by the City Chief Operating Officer is responsible for approving *Information Security Standards and Guidelines*.

5.5. *Information Security* Committee

5.5.1. The *Information Security* Committee or other IT governing body as assigned by the STAC is responsible for reviewing departments' initial requests for exemptions from the *Information Security Standards and Guidelines* and recommending modifications to the City's existing *Information Security Standards and Guidelines*, as necessary

5.6. IT Services Provider(s)

5.6.1. The City's IT services provider(s) will be responsible for providing, operating, and maintaining the City's primary *Computer Systems*, and *Email* systems, *Network Services*, and *Internet* connectivity. The IT services provider is charged with the responsibility of protecting the City's *Network Services* and *Computer Systems* from intrusion from outside sources, including the management and maintenance of firewalls

5.7. Department Directors

5.7.1. Department Directors or their designees are responsible for approving requests for *User IDs* and *User Accounts* for *Email* and *Network Services*.

5.8. *Information Security* Liaison

5.8.1. The departmental *Information Security* Liaison is the primary point of contact responsible for department compliance with the City's *Information Security Policies*.

5.9. System Administrators and System Managers

5.9.1. *System Administrators* and *System Managers* are responsible for maintaining the security and integrity of City *Computer Systems* and *Network Services*, including duties related to creating, modifying, and deleting *User IDs* or *User Accounts*, and for maintaining the confidentiality of data contained on those systems in compliance with the City's *Information Security Policies*.

5.10. IT Asset Manager

5.10.1. The department IT Asset Manager is responsible for maintaining an accurate, up-to-date inventory of all departmental IT assets, including computer hardware and software.

5.11. Supervisory Personnel

5.11.1. Supervisory Personnel are responsible for overseeing the employee's use of City *Computer Systems*, *Email* systems, and *Network Services*.

5.12. Every Individual is responsible for his/her actions and conduct in accessing or using the City's *Computer Systems*, *Network Services*, and *Email* Systems. Violation of the City's *Information Security Policies* or unauthorized or inappropriate use may result in disciplinary action.

APPENDIX

Legal References

San Diego Municipal Code, section 27.3564(b)
Administrative Regulation 45.50 - Private Use of City Labor, Equipment, Materials, and Supplies Prohibited
Administrative Regulation 90.20 - Office Telephones
Administrative Regulation 90.62 - Information and Communications Technology Acceptable Use
Administrative Regulation 90.64 - Protection of Sensitive Information and Data
Administrative Regulation 90.65 - Broadcast Email and Voice Mail

Forms Involved

Employee Acknowledgement of IT Security Policy Overview
Form IT-063 - Information Security Policy Acknowledgement

Subject Index

Computer Equipment, Security Computer Systems, Security
Electronic Mail, Security Email, Security
Internet, Security
Network Services, Security
Security – Information Technology

Distribution

All Departments (Mayoral and Non-Mayoral)

Administering Department

Department of IT

CITY OF SAN DIEGO

Information Security Policy Acknowledgement Form – City Employees

Policy Summary (pertinent excerpts from Administrative Regulation 90.63):

4.1.2. All computer files developed, created or enhanced within the scope and course of City employment, or a City third-party contractual relationship, are the property of the City of San Diego, regardless of their physical location or the form in which they are maintained. These include, but are not limited to, computer data files, documents, databases, spreadsheets, calendar entries, appointments, tasks, and notes which reside on any City Computer Systems or Computer Equipment, or the Computer Equipment of a contractor performing work for or on behalf of the City.

a. The City reserves the right to access and disclose as required or permitted by law, and as defined in the approved Information Security Standards and Guidelines, all messages and other electronic data sent over its Email systems or stored in computer files on City Computer Equipment. City-related computer files stored on non-City or personal computers must be provided upon the City's request in City standard formats.

4.1.4. Authorized access to City Computer Systems and Network Services shall be at the minimum level required for the Individual to perform and complete their assigned duties, and not at a level that allows access to information beyond the scope of that Individual's assigned duties.

4.1.5. Each Computer System or Network Services User ID must uniquely identify only one User. Generic, shared, or group User IDs are not permitted. [...] Network security groups may be used to combine Users access rights. Approved group Email accounts may be shared by multiple Users who each have unique User IDs.

4.3.1. Users must be responsible in their use of City Computer Equipment, and Network Services. Any action that may cause interference with City Computer Systems, exposes the City's Computer Systems to risk or adversely impacts the work of others in using these Computer Systems is prohibited.

4.3.2. Employees may be disciplined in accordance with standard City procedures for improperly using or knowingly allowing the improper use of the City's Computer Equipment, Network Services or Email system as stated in this regulation. Abuse of the City's Computer Systems may result in disciplinary action, up to and including termination and criminal prosecution if deemed appropriate.

4.3.4. Every end User must have a single unique User ID and a personal password which must be kept confidential and not shared with anyone else. This User ID and password will be required for access to all multi-user Computer Equipment and Network Services. User passwords must comply with the Information Security Standards and Guidelines.

4.3.5. Users accessing City Computer Systems are prohibited from gaining unauthorized access to any other non-City Computer Systems or in any way damaging, altering or disrupting the operations of those systems. Users are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

Employee/Supervisor Acknowledgement

By signing below, the employee acknowledges that he or she has been advised of the City's policies related to Information Security as provided in Administrative Regulation 90.63 ("Information Security Policy"), which has been discussed with his or her supervisor, and further acknowledges that he or she understands and agrees to comply with the provisions of the policy. Employee understands that this form will be kept as part of his or her departmental employee file, and that he or she may receive a copy, if requested. The supervisor acknowledges that he or she has discussed the policy (A.R. 90.63) with the employee named below and understands the supervisor's obligations regarding Information Security under this policy.

_____
Employee's Name (Print Legibly)

_____ _____
Employee's Signature Date Signed

_____
Supervisor's Name (Print Legibly)

_____ _____
Supervisor's Signature Date Signed

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
	90.64	2	1 of 8
PROTECTION OF SENSITIVE INFORMATION AND DATA	Effective Date May 5, 2017		

1. PURPOSE

1.1. To establish a policy to ensure the confidentiality and protection of *Sensitive Information* against unauthorized use; to establish procedures to control access to *Sensitive Information* so that it is only accessible by *Authorized Persons*; and to establish safeguards to ensure the appropriate use of *Sensitive Information* by *Authorized Persons*.

1.2. To define responsibility and procedures for granting *Authorized Persons* access to *Sensitive Information*.

1.3. To define processes by which access to *Sensitive Information* is administered and to develop control points in compliance with City policy.

2. SCOPE

2.1. This policy applies to all City employees in all City departments, including independent departments as authorized by the signing authorities below; and to City volunteers, contractors, vendors, and other individuals granted access to *Sensitive Information* under the City's control by the nature of their support or service functions.

2.2. This policy and procedures apply to all Sensitive Information created, owned, stored, managed or under the control of the City of San Diego, regardless of the media which contains the Sensitive Information, including but not limited to paper, microfilm, microfiche or any analog or digital format.

2.3. Nothing in this Administrative Regulation supersedes any stricter requirement(s) set by other authorities (i.e., local, state, and/or federal laws, rules or regulations), such as obtaining or retaining employment in a law enforcement agency; nor does this Administrative Regulation supersede any applicable, stricter rules, regulations or policies that affect access to or use of *Sensitive Information*. In such cases, the department head must ensure implementation or application of any such superseding rules, regulations or policies include adequately strong internal controls over *Sensitive Information*.

(Supersedes Administrative Regulation 90.64, Issue 1, effective July 1, 2009)

Authorized

(*Signature on File*)

CHIEF OPERATING OFFICER

3. DEFINITIONS

3.1. *Appointing Authority* - An unclassified, management-level position designated by the department head or higher who has the authority to grant permission for an employee or individual to be authorized for access to *Sensitive Information*.

3.2. *Authorized Person* - An employee or other individual who is granted permission to access or use *Sensitive Information* by an *Appointing Authority*, as approved by the *Information/Data Owner*, at the type and the *Level of Access* to the specific information required for the performance of his or her job duties.

3.3. *Authorization Acknowledgment Form* - The City's official form used to request and authorize an individual's access to or use of *Sensitive Information* (see Appendix). This form will be available on the City's Intranet site (CityNet) on the 'Forms' page.

3.4. *Information/Data Owner* - The department head or designee who is the primary recipient or manager of particular *Sensitive Information* or who has the responsibility to oversee the collection, maintenance or management of such information or data. There will only be one defined *Information/Data Owner* for any particular source of data; although other departments may collect and/or access the data. An *Information/Data Owner* may also be an *Appointing Authority*, as defined in Section 3.1 above.

3.5. *Level of Access* - The amount of *Sensitive Information* for which access is granted for any specific category or type of *Sensitive Information*, such as full access to all information related to a particular category or document, or limited access to only specific pieces of information (i.e., certain fields in a database) required for the performance of valid job duties.

3.6. *Personal Identifying Information* - Shall include information listed in California Penal Code Section 530.55(b), as amended (Sept. 2006), which reads, in pertinent part:

3.6.1. *Person* - A natural *Person*, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

3.6.2. *Personal Identifying Information* - Any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license or identification number, social security number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the *Person*, address or routing code, telecommunication identifying

information or access device, information contained in a birth or death certificate, credit card number of an individual *Person*, or an equivalent form of identification.

3.7. For the purpose of this policy, *Sensitive Information* shall mean:

3.7.1. *Personal Identifying Information* (as defined above), also including debit card number of an individual *Person*, and where home/personal address and telephone number are included and work/office address and telephone number are excluded (i.e., the City Directory is not considered *Sensitive Information*); and

3.7.2. Any information that is possessed by the City of San Diego which is not subject to the California Public Records Act (refer to Administrative Regulation 95.20), and which may be used for other than the intended purpose of such information, to cause harm to or otherwise jeopardize the City of San Diego or any individual, or used in violation of any local, state or federal law (for example the Health Insurance Portability and Accountability Act of 1996 (HIPAA)).

3.8. *Sensitive Information Custodian* - The *Person* who manages the physical or computer-based access to *Sensitive Information*; for example an office manager or records manager who controls access to locked file rooms/cabinets, or a computer systems administrator who manages the creation of user accounts and passwords to provide specific access to particular data. A *Sensitive Information Custodian* may also be an *Information/Data Owner*, as defined in Section 3.4. above.

3.9. *Type of Access* - Refers to Read Only, Write/Create, Edit/Modify, and Delete.

4. POLICY

4.1. *Sensitive Information* shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her *Appointing Authority* and approved by the *Information/Data Owner*, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.2. Contractors and vendors or other non-City employees who are authorized to access or use *Sensitive Information*, shall be required to enter into agreements stating that the individuals specified for this access and their employing Contractor/Vendor agree to be contractually bound by the terms and conditions of this policy, including personal liability, as part of their contract or agreement prior to being granted access to *Sensitive Information*.

4.3. Authorization to access or use *Sensitive Information* shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an *Authorized Person's* job duties no longer require access to or use of *Sensitive Information*, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to *Sensitive Information* extend beyond the termination of the authorizing

contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.4. The *Information/Data Owner* shall specify the type and the *Level of Access* that should be assigned to various functional roles that require access to the *Sensitive Information* based on an employee's or individual's job requirements.

4.5. *Authorized Persons* shall access or use *Sensitive Information* only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use *Sensitive Information* shall sign an *Authorization Acknowledgement Form* stating he or she has read, understands, and agrees to abide by this policy.

4.6. As a standard IT security measure, *Authorized Persons* shall not share their User ID and/or password with anyone else, and shall not have their User ID and/or password written down in any unsecured location (e.g., anywhere around their work location). "Generic" User IDs shall not be used for system access to *Sensitive Information*; each *Authorized Person* must use an assigned, unique User ID that is directly linked with the user's name. As a standard physical security measure, *Authorized Persons* shall not share their building or facility access key card or key(s) with anyone else, nor shall they allow access into secured areas by unauthorized *Persons*.

4.7. Violation of this policy, either by unauthorized *Persons* accessing or attempting to access *Sensitive Information*, or by *Authorized Persons* accessing or using *Sensitive Information* for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

4.8. Appointing Authorities shall review the list of their employees, contractors or other individuals who they have designated as *Authorized Persons* with access to *Sensitive Information*, at least semi-annually, to ensure continued authorization is warranted and to update (add, delete or modify) the authorization list appropriately.

4.9. *Information/Data Owners* shall verify and document semi-annually that the Appointing Authorities performed a thorough review of authorized users in compliance with this policy (Section 4.8.), by comparing the *Appointing Authority's* report with a list of individuals currently authorized to access the *Sensitive Information* over which the Information/Data Owner has control and authority. For internal control purposes, to maintain segregation of duties, this verification must be performed by someone other than the *Appointing Authority* who submitted the semi-annual review of *Authorized Persons*. All discrepancies shall be reported back to the impacted *Appointing Authority* for

appropriate corrective action. *Information/Data Owners* shall retain records of such reviews and actions for the period of time set within the citywide or departmental Records Retention Schedule as approved by the City Clerk.

4.10. *Sensitive Information* stored in City computer systems shall be secured and maintained in accordance with applicable provisions of the Information Security Guidelines and Standards, as amended.

4.11. *Sensitive Information* stored in paper or other non-digital formats shall have appropriate physical security, and access to such information shall also comply with Administrative Regulation 95.10 for validating the identity of the individual requesting authorized access.

4.12. Upon the discovery of any breach of the protection of *Sensitive Information* through the accidental, inadvertent or purposeful release of such information to any unauthorized *Persons*, the *Person* discovering such breach should immediately notify the *Information/Data Owner* or their *Appointing Authority*, and, if the information was stored on City computer systems, also notify the Chief Information Security Officer in the Department of Information Technology.

4.12.1. Depending on the nature and scope of such breach and release of information, additional notifications must comply with applicable state and federal regulations.

4.12.2. The Information/Data Owner, in coordination with the Chief Information Security Officer from the Department of Information Technology (if applicable), should immediately take whatever steps are deemed necessary to stop any further breach of the protected information and to minimize any potential or actual losses or damages to the City of San Diego.

5. RESPONSIBILITY

5.1. Supervisor

5.1.1. When an employee's, volunteer's or contractor's job duties require access to or use of *Sensitive Information*, the immediate supervisor will complete an Authorization Acknowledgment Form. In addition, the supervisor must ensure that the proper system access/account request form and process is followed for the specific computer system where the *Authorized Person* needs access, specifying the nature of the job duties and the level and *Type of Access* or use requested. The supervisor will ensure the accuracy and completeness of information on the forms. After obtaining the employee's signature, the acknowledgement and request forms will be routed to the *Appointing Authority* for approval. Likewise, when an employee's, volunteer's or contractor's job duties change such that access to or use of *Sensitive Information* is no longer needed, the immediate supervisor will notify both the

Appointing Authority and the *Information/Data Owner*, as soon as possible (no more than five (5) business days).

5.2. *Authorized Person* (employee, volunteer, contractor, vendor or other individual being authorized for access).

5.2.1. Any *Person* being given access to *Sensitive Information* must sign the *Authorization Acknowledgement Form* stating he or she has read, understands, and agrees to comply with this policy for access or use and protection of such information. A copy of the final, approved form shall be kept in the employee's departmental personnel file, as the *Appointing Authority's* record; or for volunteers, on file with the department where assigned; or for a contractor, on file with the contract manager.

5.3. Department *Appointing Authority*

5.3.1. The Department *Appointing Authority* having management control over the employee, volunteer, contractor Vendor or other individual seeking authorization to access *Sensitive Information*, shall review the Authorization Acknowledgement and system access/account request forms for appropriateness of the job functions for the type and *Level of Access* requested while considering appropriate segregation of duties, and ensure the forms are signed by both the individual and supervisor.

5.3.2. The Department *Appointing Authority* will sign either approval or denial of the request, providing the reasons for any denial, and route the approved request form to the appropriate *Information/Data Owner*(s), or route a denied form back to the supervisor. Appointing Authorities shall maintain a copy of all authorization forms they approve, including those for non-City employees (i.e., volunteers and contractors). Any changes reported in the job duties of *Authorized Persons* which require a change in the access to or use of *Sensitive Information* must be immediately communicated to the *Information/Data Owner* to initiate the appropriate change in access. The semi-annual reviews should take place in May and November each year. The *Appointing Authority* will submit documentation of each review to the *Information/Data Owner* and these records will be retained by the department for the period of time set by the citywide or departmental Records Retention Schedule as approved by the City Clerk.

5.4. Information/Data Owner (owner of the information, regardless of its format or mechanism of access, [i.e., computerized system, hard copy file, etc.])

5.4.1. The Information/Data Owner for each different source of *Sensitive Information* covered by an approved access request form will review each request to ensure the type and *Level of Access* requested is appropriate for the job functions of the individual seeking access. Upon confirmation of the business need to have access

to *Sensitive Information*, the Information/Data Owner will sign approval to grant access, and may modify the type or *Level of Access* granted, as he or she deems necessary and appropriate, in consultation with the requesting *Appointing Authority*. The Information/Data Owner will initiate any further actions necessary to grant access to the *Authorized Person* (such as any computer system access processes). *Information/Data Owners* will maintain a list of individuals currently authorized access to their *Sensitive Information* and provide such list to the appropriate *Appointing Authority* for semi-annual review at the end of April and October each year

5.5. *Sensitive Information Custodian* (Administrator of the format and/or mechanism of access [i.e., computerized system or hard copy file] for the given information)

5.5.1. The *Authorized Person's* access to the identified *Sensitive Information* will be set up following the established procedures either in the IT Security Guidelines and Standards for access to electronic or digital data or following departmental internal controls for paper or physical records, based on the nature (media/format) of the *Sensitive Information*.

5.6. Department of Information Technology

5.6.1. Annually review this policy for any necessary updates or revisions, taking into account changes in City organization and IT systems. Maintain the list of *Information/Data Owner*s and update it annually. Maintain the necessary correlation between this policy and other IT security policies and/or regulations. Ensure City third-party vendors who have access to this data comply with this and other IT security policies. The Department of Information Technology is also responsible for ensuring that the requirements of this policy are communicated to all employees at least annually, using citywide and/or departmental training or communication channels.

5.7. Purchasing & Contracting Department

5.7.1. Ensure that this policy is included as an Addendum to or within the Terms and Conditions of signed contracts or agreements, for all contracts and/or agreements that include a contractor's or vendor's need to access or use the City's *Sensitive Information*.

SUBJECT	Number	Issue	Page
	90.64	2	8 of 8
PROTECTION OF SENSITIVE INFORMATION AND DATA	Effective Date May 5, 2017		

APPENDIX

Legal References

Civil Service Rules and City Personnel Manual
Civil Service Rules, Definitions (p.l), "Appointing Authority"
Civil Service Rule XI, "Resignation, Removal, Suspension, Reduction in Compensation, Demotion"
Personnel Manual, Index Code A-3, "Improper Use of City Resources"
Personnel Manual, Index Code G-1, "Code of Ethics and Conduct"
Administrative Regulation 45.50 - Private Use of City Labor, Materials, Equipment and Supplies Prohibited
Administrative Regulation 90.63 - Information Security Policy
Administrative Regulation 95.10 - Identification of City Employees and Controlled Access to City Facilities
Administrative Regulation 95.20 - Public Records Act Requests and Civil Subpoenas; Procedures for Furnishing Documents and Recovering Costs
Administrative Regulation 95.60 - Conflict of Interest and Employee Conduct
IT Security Guidelines and Standards
Employee Performance Plans, Ethics and Integrity Section
Applicable California State Laws
Applicable Federal Laws

Forms Involved

Form DoIT-010A, "*Sensitive Information* Authorization Acknowledgement-City Employees"
Form DoIT-010B, "*Sensitive Information* Authorization Acknowledgement-City Volunteers"
Form DoIT-010C, "*Sensitive Information* Authorization Acknowledgement-City Contractors/Vendors"

Subject Index

Sensitive Information
Sensitive Data Information Security
Protection of *Sensitive Information*

Distribution

All Departments (Mayoral and Non-Mayoral)

Administering Department

Department of Information Technology

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form - City Employees

Authorized Person (City Employee requesting authorized access to Sensitive Information):

Name (Printed)	*Job Classification*	*Network (AD) Login/User ID*
Department / Division		
Mail Station	*Office Phone*	*Office FAX*
Supervisor's Name (Printed)	*Supervisors Phone*	

Policy Summary (pertinent excerpts from Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. [...]

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above employee acknowledges the he or she has been provided a full copy of A.R. 90.64 ("Protection of Sensitive Information and Data"), which has been discussed with his or her supervisor, and further acknowledges that he or she has read, understands, and agrees to comply with the provisions of the policy. Employee understands that this form will be kept as part of his or her permanent employee file, and that he or she may receive a copy, if requested. The supervisor acknowledges that he or she has discussed the policy with the above employee and understands the supervisor's obligations regarding employee's access to Sensitive Information under this policy.

_____ _____

Employee's Signature Date Signed

_____ _____

Supervisor's Signature Date Signed

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form- City Volunteers

Authorized Person (City Volunteer requesting authorized access to Sensitive Information):

Name (Printed)	*Volunteer Assignment*	*Network (AD) Login/User ID*
City Department / Division (where assigned as volunteer)		
Work Location		*Contact Phone*
City Supervisor's Name (Printed)	*City Supervisor's Phone*	*City Supervisor's Mail Station*

Policy Summary (pertinent excerpts from Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role Job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to Sensitive Information extend beyond the termination of the authorizing contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above City Volunteer acknowledges the he or she has been provided a full copy of A.R. 90.64 ("Protection of Sensitive Information and Data"), which has been discussed with the City Supervisor, and further acknowledges that he or she has read, understands, and agrees to comply with the provisions of the policy. City Volunteer understands that this form will be kept on file with the City Department, and that he or she may receive a copy, if requested. The City Supervisor acknowledges that he or she has discussed the policy with the above volunteer and understands the supervisor's obligations regarding the volunteer's access to Sensitive Information under this policy.

_____ _____

Volunteer's Signature Date Signed

_____ _____

City Supervisor's Signature Date Signed

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form- City Contractors/Vendors

Authorized Person (City Contractor/Vendor requesting authorized access to Sensitive Information):

Name (Printed)	*eMail Address*	*Network (AD) Login/User ID*
Company/Organization		*Contractor/Vendor Office Phone*
City Department (managing contract)		*Contractor/Vendor Office FAX*
City Contract Manager's Name (Printed)	*City Contract Manager'8 Phone*	*City Contract Manager's Mail Sta.*

Policy Summary (pertinent excerpts from City Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to Sensitive Information extend beyond the termination of the authorizing contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above City Contractor/Vendor acknowledges the he or she understands that the Terms and Conditions of the underlying City Contract contain the provisions of the full policy stated above, and he or she agrees to comply with such contract provisions. City Contractor/Vendor understands that this form will be kept on file with the underlying contract documents in the City Purchasing & Contracting Department, and that he or she may receive a copy, if requested. The City Contract Manager acknowledges that he or she has discussed the contract Terms and Conditions related to this policy with the above Contractor/Vendor and understands the supervisor's obligations regarding the Contractor's/Vendor's access to the City's Sensitive Information under this policy.

_____ _____

Contractor's/Vendor's Signature Date Signed

_____ _____

City Contract Manager's Signature Date Signed

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
	90.68	1	1 of 6
PROCUREMENT OF TECHNOLOGY SOLUTIONS	Effective Date April 14, 2021		

1. PURPOSE

1.1. This Administrative Regulation (A.R.) establishes the Department of Information Technology (Department of IT), headed by the Chief Information Officer (CIO), as the authority which defines and enforces *Information Technology Governance*, including citywide procedures for procuring, implementing, and maintaining *Information Systems*.

1.2. This A.R. will ensure that as activities occur throughout the City's *Information Systems* lifecycle, they are documented and reviewed to ensure they conform with industry best practices.

1.3. This A.R. adheres to best practices in the Information Technology Infrastructure Library framework while using common terminology instead of the technical definitions to promote a broader understanding of the process.

2. SCOPE

2.1 This A.R. applies to all City departments and employees who engage in the activity of procuring, implementing, and maintaining information systems for the City of San Diego.

3. DEFINITIONS

3.1. *Change Advisory Board* – a group composed of *IT Technical Leads* that can include individuals from the *Initiating Department* who assess, prioritize and schedule the changes required for deploying the *Information System*.

3.2. *Demand* – a request for an *Information System* to serve a business need for an *Initiating Department*.

3.3. *Department Lead* – a member of the *Initiating Department* who will steer the process to implement a new or updated *Information System*.

3.4. *Gate* – a checkpoint that is part of *Information Technology Governance* to ensure that a new or updated *Information System* aligns with the City's business needs, meets the City's technological requirements, follows an efficient implementation process, and is rolled out effectively. There are *Gates* at each stage of the *Information Technology Governance* process, for example, the *Demand Gate*, the Project Planning *Gate*, the Design Review *Gate*, and the Change Management

Gate. See Appendix 1 for a more detailed description of each *Gate*.

3.5. *Information Technology Governance (IT Governance)* – a process used by organizations worldwide that provides a formal framework to ensure that investments into *Information Systems* align digital strategy with business strategy.

3.6. *ITIL* - The Information Technology Infrastructure Library (ITIL) is the most widely recognized framework for IT best practices and provides comprehensive, practical and proven guidance for establishing an effective service management system. See https://www.axelos.com for additional detailed information on ITIL.

3.7. *Information Systems* – Software, hardware, data, cloud services, and procedures that integrate information technology solutions and business processes to meet the needs of City departments and include services that require a City user to login to an online account or access an *Information System*.

3.8. *Initiating Department* – The department implementing a new or significantly updated *Information System*.

3.9. *IT Liaison* – a representative from the Department of IT who helps guide *Department Leads* and *Project Managers* through the *Information Technology Governance* process to procure and implement technology solutions.

3.10. *IT Technical Leads* – individuals in the Department of IT, the *Initiating Department* or *Information System* vendors. They can include the CIO, deputy directors, managers, *Information Systems* analysts or cyber security personnel who provide input as part of the Design Review and Change Management *Gates*.

3.11. *Project* – after a demand is approved by the Department of IT, this is the status of an *Information System* before it is implemented. A *project* is a concerted effort to deliver an *Information System*, bounded by time, that has a defined outcome and deliverables, a deadline, and a budget limiting number of people, supplies and capital.

3.12. *Project Manager* – an individual employed by the City of San Diego or a contractor responsible for planning and coordinating the steps necessary and leading the project team to implement new or changing *Information Systems*. The project manager must have a project management professional (PMP) certification or have successfully run projects within the City that have followed a recognized project management methodology. *The Project Manager* can sometimes be the same individual as the *Department Lead.*

3.13. *Project Sponsor* – typically a management-level individual at the City. During

the planning and execution stages of the project, the sponsor acts as a champion for the project at an appropriate level with key stakeholders. The Sponsor ensures that the business case and scope for the *Information System* are in alignment with the business need.

3.14. *Tech Alignment Review Form* – A checklist provided by the Department of IT used to ensure that a new or upgraded *Information System* meets cybersecurity standards and is compatible with other systems in the City.

4. POLICY

4.1. City departments shall follow the *Information Technology Governance* process and provide justification for any new or significantly updated *Information System* to ensure compliance with procurement and implementation requirements.

4.2. When an *Initiating Department* wants to procure a new or significantly updated *Information System* or services that rely on *Information Systems* to help solve a business need, its *Department Lead* or *Project Sponsor* shall submit his or her ideas to the *IT Liaison* for review.

4.3. *Department Leads* or *Project Sponsors* must ensure that they have received financial approvals for the *Project* before beginning the *IT Governance* process.

4.4. The *IT Liaison* will then meet with the *Project Sponsor* and *Department Lead* to ensure they fully understand the requirements for the *Information System.*

4.5. The *IT Liaison* will research potential solutions, determine significant risks, technological dependencies, or other potential issues with the desired solution before providing a recommendation to a *Department Lead.*

4.6. The *Department Lead* shall work with the Purchasing and Contracting Department to determine whether a competitive bidding process is needed or if a sole source contract is required to procure the desired solution.

4.7. Prior to choosing an *Information System,* the *Department Lead* shall work closely with the *IT Liaison* to ensure the solution meets the requirements in the *Tech Alignment Review Form.*

4.8. Once the *Tech Alignment Review Form* has been completed, the *IT Liaison* will enter a *demand* for the selected *Information System* into an IT Governance system used to track *Projects* used by the Department of IT.

4.9. The *IT Liaison* will present the proposed *Information System* at the *Demand Gate* and seek approval for the project from the *IT Technical Leads.*

4.10. A *Project Manager* must be brought on to the *project* once the *demand* is approved and work alongside the *Department Lead* to develop a plan for the implementation of the *Information System*.

4.11. The *Project Manager* will facilitate the Project Planning *Gate*, where the *IT Liaison* will review the plan and provide feedback and recommendations with the *Department Lead* and the *Project Sponsor* present.

4.12. Upon plan approval by the *IT Liaison*, the *Project Manager* will then facilitate the Design Review *Gate*, where *IT Technical Leads* and the *IT Liaison* will provide recommendations to the *Project Manager* or *Project Manager's* designee about the technical implementation of the proposed *Information System*.

4.13. The *Project Manager* or their designee will participate in the Change Management *Gate* to explain how the *Information System* will be deployed. This can include support plans, communication plans, training dates or the creation of written guides.

4.14. Once the *Change Advisory Board* has made deployment recommendations, *the Project Manager* will take the appropriate steps to deploy the *Information System* to users.

5. RESPONSIBILITIES

5.1 Department Lead

5.1.1. The *Department Lead* represents the *Initiating Department* as the individual responsible and accountable for the appropriate vetting, procurement, and implementation of their desired *Information System*. They are accountable for ensuring all process steps are followed and completed.

5.1.2 The *Department Lead* will ensure a qualified *Project Manager* is managing the *Project*.

5.1.3. The *Department Lead* must complete the *Information Technology Governance* process.

5.2. Project Manager

5.2.1. The *Project Manager* is responsible for the execution of the entire *Project* to implement the desired *Information System*.

5.2.2. The *Project Manager* must complete the *Information Technology*

Governance process.

5.3. IT Liaison

5.3.1. The *IT Liaison* is responsible for assisting the *Department Lead* through the process to procure and/or implement new or updated *Information Systems*.

5.3.2. The *IT Liaison* assists the *Department Lead* in identifying any existing *Information Systems* that may meet the business requirements.

5.3.3. The *IT Liaison* assists the *Department Lead* and *Project* Manager to ensure all *Gate* requirements have been fulfilled as outlined in the IT Governance Overview (Attachment 1).

5.3.4. The *IT Liaison* participates in the *Gates* as required.

5.3.5. The *IT Liaison* maintains and develops checklists that will guide the *Department Lead* and/or *Project Manager* between each *Gate.*

5.3.6. The *IT Liaison* provides appropriate checklists to be completed by the *Department Lead* and/or *Project Manager.*

5.4. IT Technical Leads

5.4.1. The *IT Technical Leads* participate in the *Demand* and Design Review *Gates* to provide feedback and recommendations about the technical implementation of the proposed *Information System.*

5.5. Project Sponsor

5.5.1. A *Project Sponsor* is mandatory for all projects that are valued at $50,000 or more. (Project Sponsor training is available on Success Factors and is required prior to fulfilling this role).

5.5.2. The *Project Sponsor* leads the project through the engagement or selection process until the *Demand* is approved.

5.5.3. The *Project Sponsor* acts as a spokesperson to higher-level management to gather support throughout the organization and promote the benefits that the project will bring.

5.5.4. Once the project begins, the *Project Sponsor* reviews the *Project* with the *Department Lead* and/or *Project Manager* at the Project Planning *Gate.*

5.5.5. The *Project Sponsor* provides guidance on *Project* scope, timeline, cost, risks, assumptions, constraints, and dependencies.

APPENDIX

Legal References

Administrative Regulation 90.63 – Information Security Policy

Forms

Attachment 1 –Information Technology Governance Overview

Subject Index

IT Governance Process for Procurement of Information Systems
Project Management Methodology

Administering Department

Information Technology

ATTACHMENT 1

Below is an overview of each gate in the Information Technology Governance process.

Demand Gate: Entering a Demand is the beginning of the IT Governance process. During this gate, the Department of IT reviews demands to determine the downstream technological impacts and evaluates technical risks to ensure selected system is supportable by the City's technical landscape.

Project Planning Gate: During the Project Planning Gate Review, the IT Liaisons will review all planning documentation. IT Liaisons will make recommendations based on the meeting on the project approach the project team plans to use to deliver the intended scope. Reviewing planning documentation is a proven best practice for projects to ensure successful implementation.

Design Review Gate: The use of Design Reviews is proven best practice in systems development projects in ensuring successful implementation of applications, networks, security features or data centers. During the standard IT Governance process, IT Technical Leads will be reviewing each demand to determine if a Design Review is required.

Change Management Gate: The purpose of the change management process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services. The Department of IT Change Management process maximizes value by driving faster changes and with higher success rates. Change management's general practice, focuses highly on system reliability and protects business continuity, while minimizing disruption.