

AGREEMENT FOR MANAGEMENT OF INFORMATION TECHNOLOGY SERVICES

This Agreement for Management of Information Technology Services (the "Agreement") is made and entered into by and between the Wheaton Park District (the "Park District"), an Illinois unit of local government, and Advanced Intelligence Engineering ("Vendor"), an Illinois corporation, which hereinafter may be referred together as the "Parties" or individually as a "Party."

WHEREAS, the Park District desires Vendor to perform certain management of information technology services for the Park District, as detailed in the Park District's Request for Proposal dated July 1, 2021, attached and incorporated as Exhibit A ("RFP") and Vendor's Proposal dated August 1, 2021, attached and incorporated as Exhibit B (the "Proposal"), and Vendor desires to provide said services to the Park District described hereunder based on and subject to the terms and conditions set forth in this Agreement.

Section 1: MANAGEMENT OF INFORMATION TECHNOLOGY SERVICES.

Vendor shall provide the management of information technology services detailed in the RFP and the Proposal (hereinafter referred to as the "Services"). The Park District may desire to have Vendor render additional services in connection with this Agreement other than those expressly provided for in the Contract Documents (defined below). Any additional services shall not commence unless authorized in writing by the Park District. Vendor shall perform the additional services in accordance with the standards for performance of the Services under this Agreement.

Section 2: CONTRACT DOCUMENTS.

The Contract Documents consist of this Agreement between the Park District and Vendor, the RFP, the RFP response Proposal, and the Master Services Proposal dated December 29, 2021 attached as Exhibit C ("MSP"). All of the terms, conditions and specifications contained in the Contract Documents are incorporated herein. In the event of any conflict between any provision of the Proposal and this Agreement, the terms of this Agreement shall control.

Section 3: TERM OF AGREEMENT.

The term of this Agreement shall commence on January 1, 2022 and, unless terminated earlier as provided herein, shall expire on December 31, 2025 (the "Term").

Section 4: SCHEDULE FOR PERFORMANCE OF VENDOR'S SERVICES.

Vendor's Services shall be performed in a timely manner and in accordance with the Contract Documents, as may be amended by the Parties in writing or in accordance with this Agreement.

Section 5: PERFORMANCE OF WORK.

Vendor agrees to perform faithfully, industriously, and to the best of Vendor's ability, experience, and talents, in accordance with generally accepted standards of professional skill and care among recognized industry experts engaged in similar services, all of the duties described in the Contract Documents or as otherwise required by the express and implicit terms of this Agreement or greater generally recognized industry standards

in order to produce a first class work product and services of the type and scope contracted for under this Agreement, to the reasonable satisfaction of the Park District. Vendor shall perform all of its duties hereunder according to the Park District's requirements and procedures and in compliance with all applicable national, federal, state, county and local laws, regulations, codes, ordinances, orders and with those of any other body having jurisdiction. The Park District shall be the sole judge of whether Vendor's duties are performed satisfactorily. The duties of Vendor may be specified and modified from time to time by the Park District in writing.

Section 6: PAYMENT FOR SERVICES.

The Park District agrees to compensate Vendor for providing the Services in accordance with the Pricing Schedule outlined in the MSP. Payment shall be made by the Park District to the Vendor upon the Park District's receipt of an invoice itemizing the Services properly performed, as determined by the Park District, for the period covered by the invoice. The Vendor will invoice the Park District on a monthly basis. Payments of all invoices, and any late payment penalties, shall be governed by the Local Government Prompt Payment Act (5 ILCS 505/1 *et seq.*). Each invoice shall include a description of the Services completed to the date of the invoice and, with respect to any additional services included, the nature of the additional services as listed in the Proposal, the date those additional services were approved by the Park District, and the number of hours or portion thereof that were expended by each such person in the performance of the additional services.

Section 7: PAYMENT FOR ADDITIONAL SERVICES.

For the proper performance of any additional services, first approved in writing by the Park District, the Park District shall compensate Vendor in accordance with the Pricing Schedule outlined in the MSP.

Section 8: OWNERSHIP OF INSTRUMENTS OF SERVICE.

Any and all documents, including but not limited to, any plans, notes, analysis, and any other documents prepared by Vendor in the performance of its Services under this Agreement (hereinafter "Instruments of Service") is work done for hire and ownership of such Instruments of Service vests in the Park District. The Park District retains exclusive property rights including all common law, statutory, federal and other reserved rights in the Instruments of Services, including copyrights.

Section 9: PARK DISTRICT'S MARKS.

The "Park District's Marks" shall mean the Park District's name and trade or service marks, labels, designs, logos, trade names, product identifications, artwork and other symbols, devices, copyright and intellectual property rights directly associated with the Park District or any program, facility, special event of business of the Park District, whether existing on the date of execution of this Agreement or created thereafter. The Park District's Marks are and shall remain the Park District's property.

-
- a) Vendor is hereby authorized to use the Park District's Marks for the Services during the Term of this Agreement, provided the Park District shall have the right to approve all such uses in writing in advance.

- b) Vendor shall not use or permit the use of the Park District's Marks unless such use is authorized by this Agreement or such use is permitted by the prior written consent of the Park District.
- c) The right to use the Park District's Marks is non-exclusive, non-assignable and nontransferable. All use by Vendor of the Park District's Marks shall inure solely to the benefit of the Park District.

Section 10: CONFIDENTIALITY.

The Parties agree that they will not permit the duplication or disclosure of any information designated in advance by the other Party as "Confidential and Proprietary" to any person (other than its own employee, agent, or representative who must have such information for the performance of that Party's obligations hereunder) unless such duplication, use or disclosure is specifically authorized in writing by the other Party or is required by law. "Confidential and Proprietary" information does not include ideas, concepts, know-how or techniques related to information that, at the time of disclosure, is in the public domain unless the entry of that information into the public domain is a result of any breach of this Agreement. Likewise, "Confidential and Proprietary" information does not apply to information that is independently developed, already possessed without obligation of confidentiality, or rightfully obtained from a third party without an obligation of confidentiality.

Section 11: TERMINATION.

This Agreement may be terminated or suspended by the Park District, in whole or in part, for convenience and without cause upon thirty (30) days prior written notice. This Agreement may be terminated or suspended by Vendor, in whole or in part, for convenience and without cause upon thirty (30) days prior written notice. In the event of termination, Vendor will be paid for all approved Services properly rendered to the date of termination, and upon such payment, all obligations of the Park District to Vendor under this Agreement shall cease. Furthermore, in the event of such termination, Vendor shall promptly deliver to the Park District all Instruments of Service generated in the performance of its Services under this Agreement up to and including the date of termination.

The Park District shall have the right to terminate this Agreement immediately: i) upon Vendor's failure to cure or to commence to cure any breach or default of its obligations hereunder within five (5) days after written notice from the Park District of Vendor's said breach or default; ii) if Vendor ceases operation without a successor approved by the Park District in accordance with Section 18; or iii) upon Vendor's violation of any federal or state laws, or local regulations or ordinances. Upon termination due to Vendor's breach of this Agreement, Vendor shall pay the Park District all reasonable costs incurred by the Park District due to said breach, including the cost of obtaining replacement Services.

Section 12: INSURANCE.

Vendor shall procure, keep in full force and effect, and maintain at its sole cost and expense, for the duration of this Agreement, insurance against claims for injuries to persons or damages to property, intellectual property claims, and any third party intellectual property claims, which may arise from or in connection with the performance of the Services hereunder by the Vendor, its agents, representatives, employees, or subcontractors. The Park District shall be named as the certificate holder and the Park District, its elected and appointed officials, employees, agents and volunteers shall be named as additional insureds on the Vendor's Commercial General Liability policy on the Certificate of Insurance.

Vendor shall obtain insurance of the types and in the minimum amounts listed below.

A. Commercial General and Umbrella Liability Insurance. Vendor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than \$1,000,000 for each occurrence. If such CGL insurance contains a general aggregate limit, it shall apply separately to this project/location. CGL insurance shall be written on Insurance Services Office (ISO) occurrence form CG 00 01 10 93, or a substitute form providing equivalent coverage, and shall cover liability arising from premises, operations, independent contractors, products-completed operations, personal injury and advertising injury, and liability assumed under an insured Agreement (including the tort liability of another assumed in a business Agreement). The Park District, its elected and appointed officials, employees, agents and volunteers shall be included as an insured under the CGL, using ISO additional insured endorsement CG 20 10 or a substitute providing equivalent coverage, and under the commercial umbrella, if any. This insurance shall apply as primary insurance with respect to any other insurance or self-insurance afforded to the Park District. There shall be no endorsement or modification of the CGL limiting the scope of coverage for liability arising from pollution, explosion, collapse, or underground property damage.

B. Professional Liability Insurance. Vendor shall maintain professional liability and, if necessary, commercial umbrella liability insurance with a limit of not less than \$1,000,00 for each wrongful act arising out of the performance or failure to perform professional services and \$1,000,000 aggregate.

C. Business Auto and Umbrella Liability Insurance. Vendor shall maintain business auto liability and, if necessary, commercial umbrella liability insurance with a limit of not less than \$1,000,000 for each accident. Such insurance shall cover liability arising out of any auto including owned, hired and non-owned autos. Business auto insurance shall be written on Insurance Services Office (ISO) form CA 00 01, CA 00 05, CA 00 12, CA 00 20, or a substitute form providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage equivalent to that provided in the 1990 and later editions of CA 00 01.

D. Workers Compensation Insurance. Vendor shall maintain workers compensation as required by statute and employers liability insurance. The commercial umbrella and/or employers liability limits shall not be less than \$1,000,000 for each accident for bodily injury by accident or for each employee for bodily injury by disease. If the Park District has not been included as an insured under the CGL using ISO additional insured endorsement CG 20 10 under the Commercial General and Umbrella Liability Insurance required in this Agreement, Vendor waives all rights against the Park District and its officers, officials, employees, volunteers and agents for recovery of damages arising out of or incident to Vendor's work.

E. General Insurance Provisions

(1) Prior to beginning any services, Vendor shall furnish the Park District with a certificate(s) of insurance and applicable policy endorsement(s), executed by a duly authorized representative of each insurer, showing compliance with the insurance requirements set forth above. All certificates shall provide for thirty (30) days' written notice to the Park District prior to the cancellation or material change of any insurance referred to therein. Written notice to the Park District shall be by certified mail, return receipt requested.

(2) Acceptability of Insurers. For insurance companies which obtain a rating from A.M. Best, that rating should be no less than A VII using the most recent edition of the A.M. Best's Key Rating Guide. If the Best's rating is less than A VII or a Best's rating is not obtained, the Park District has the right to reject insurance written by an insurer it deems unacceptable.

(3) Cross-Liability Coverage. If Vendor's liability policies do not contain the standard ISO separation of insureds provision, or a substantially similar clause, they shall be endorsed to provide cross-liability coverage.

(4) Deductibles and Self-Insured Retentions. Any deductibles or self-insured retentions must be declared to the Park District. At the option of the Park District, Vendor may be asked to eliminate such deductibles or self-insured retentions as respects the Park District, its officers, officials, employees, volunteers and agents or required to procure a bond guaranteeing payment of losses and other related costs including but not limited to investigations, claim administration and defense expenses.

Section 13: INDEMNIFICATION.

To the fullest extent permitted by law, Vendor, its officers, directors, employees, volunteers and agents shall indemnify and hold harmless the Park District and its officers, officials, employees, volunteers and agents from and against all claims, suits, damages, causes of action, judgment, losses, costs and expenses, including but not limited to legal fees (attorney's and paralegals' fees and court costs), arising from or in connection with the Services performed by Vendor, its officers, directors, employees, volunteers and agents under this Agreement, including but not limited to any accident, injury, damage, property loss or theft, except to the extent caused by the negligence or omission of the Park District, or arising from or in any way connected with any act, omission, wrongful act or negligence of Vendor, its officers, director, employees, volunteers and agents. Such obligation shall not be construed to negate, abridge, or otherwise reduce any other right or obligation of indemnity which would otherwise exist as to the Park District. Vendor shall similarly protect, indemnify and hold and save harmless the Park District, its officers, officials, employees, volunteers and agents against and from any and all claims, costs, causes, actions and expenses including but not limited to legal fees, incurred by reason of Vendor's breach of any of its obligations under, or Vendor's default of, any provision of this Agreement.

Section 14: NO INFRINGEMENT.

Vendor warrants that the products used for the Services and any parts thereof will not infringe on any copyrights, trademark rights, patent rights, trade secrets or other rights of any third party. Vendor agrees to indemnify, defend and hold Park District harmless from and against any loss, cost, damage, liability, or expense (including attorney's fees and other reasonable litigation expenses) suffered or incurred by Park District in connection with any such infringement claim by any third party, provided however that Park District permits Vendor all available information, assistance and authority to enable Vendor to do so. Vendor further warrants that if Park District is enjoined from using any products provided by Vendor due to an actual or claimed infringement of any patent, trademark, or copyright or other property right or for any other reason, then at Vendor's option, Vendor shall promptly either: (i) procure for the Park District, at Vendor's expense, the right to continue using said product; or (ii) replace or modify the product, at Vendor's expense, so that the product becomes non-infringing.

Section 15: NO LIABILITY.

The Park District is not responsible or liable for any injury, damages, loss or costs sustained or incurred by any person including, without limitation Vendor's employees, or for any damage to, destruction, theft or misappropriation of any property, relating in any way, directly or indirectly, to Vendor's Services and obligations under this Agreement. The Park District is not liable for acts or omissions of Vendor or any of Vendor's employees, subcontractor's, agents or other persons purporting to act at the direction or request, on behalf, or with the implied or actual consent, of Vendor.

Section 16: INDEPENDENT CONTRACTOR.

The relationship between Vendor and the Park District is that of an independent contractor. Vendor shall supply all personnel, equipment, materials, and supplies at its own expense, except as specifically set forth herein. Vendor shall not be deemed to be, nor shall it represent itself as, employees, partners, or joint venturers of the Park District. Vendor is not entitled to workers' compensation benefits or other employee benefits from the Park District and is obligated to directly pay federal and state income tax on money earned under this Agreement.

Section 17: NO THIRD PARTY BENEFICIARY.

This Agreement is entered into solely for the benefit of the contracting Parties, and nothing in this Agreement is intended, either expressly or impliedly, to provide any right or benefit of any kind whatsoever to any person and/or entity who is not a party to this Agreement or to acknowledge, establish or impose any legal duty to any third party. Nothing herein shall be construed as an express and/or implied waiver of any common law and/or statutory immunities and/or privileges of the Park District and/or Vendor, and/or any of their respective officials, officers and/or employees.

Section 18: NON-ASSIGNMENT.

Vendor shall not assign any of its obligations under this Agreement without the Park District's written consent, which may be granted or withheld in the Park District's sole discretion.

Section 19: NO CONFLICT OF INTEREST.

Vendor represents and warrants that Vendor does not have a business interest or a close family relationship with any Park District officer or employee who was, is, or will be involved in Vendor selection, negotiation, drafting, signing, administration, or evaluating Vendor's performance. As used in this section, the term "Vendor " shall include any employee of the Vendor who was, is, or will be involved in the negotiation, drafting, signing, administration, or performance of the Agreement. As used in this section, the term "close family relationship" refers to the following: spouse or domestic partner; any dependent parent, parent-in-law, child, son-in-law, or daughter-in-law; or any parent, parent-in-law, sibling, uncle, aunt, cousin, niece or nephew residing in the household of a Park District officer or employee described above.

Section 20: KEY PERSONS/NO SUBCONTRACTS.

Vendor shall not transfer or reassign any individual designated in this Agreement as essential to performing

the Services, without the express written consent of the Park District, which consent shall not be unreasonably withheld. If, during the Term of this Agreement, any such individual leaves the Vendor's employment, Vendor shall present to the Park District one or more individual(s) with greater or equal qualifications as a replacement, subject to the Park District's approval, which shall not be unreasonably withheld. The Park District's approval shall not be construed to release Vendor from its obligations under this Agreement.

Furthermore, Vendor shall not subcontract with any third party to perform any of the Services and understands and agrees that the Park District is hiring Vendor for its knowledge and experience in the field of management of information technology services.

Section 21: DESIGNATED REPRESENTATIVES.

The Park District hereby designates **Michael Benard and Sandra Simpson** as the Park District's representative ("Park District's Representative") for all matters for the Park District under this Agreement and with respect to the administration of this Agreement. The Park District's Representative shall be available to Vendor at all reasonable times for consultation with Vendor. Vendor shall confirm to the Park District in writing any decision made by the Park District's Representative. Vendor hereby designates **Geoff Pearson and Jeremy Wills** as the Vendor's Representative ("Vendor's Representative") for all matters for Vendor under this Agreement and with respect to the Services to be performed by Vendor for the Park District. Vendor's Representative shall be available to the Park District at all reasonable times for consultation with the Park District's Representative. The Park District may conclusively rely on the decisions made by Vendor's Representative, including those which modify this Agreement. Either Party may change its Representative under this Agreement by giving notice to the other Party as provided hereunder.

Section 22: DISPUTES.

Any dispute or misunderstanding that may arise under this Agreement concerning Vendor's performance shall first be resolved through negotiations, if possible, between each Party's Designated Representative as specified in Section 21 of this Agreement. If such officials do not agree upon a decision within a reasonable period of time, the Parties may pursue other legal means to resolve such disputes.

Section 23: CHOICE OF LAW AND VENUE.

This Agreement is governed by the laws of the State of Illinois. Any suit or action arising under this Agreement shall be commenced in the Circuit Court of DuPage County, Illinois. In any suit or action arising under this Agreement, the prevailing Party shall be entitled to an award of reasonable attorneys' fees and costs of litigation.

Section 24: COMPLIANCE WITH LAWS.

Vendor shall comply with all federal, state and local laws, rules and regulations and shall obtain at Vendor's own cost and expense all permits and licenses which may be required in order for Vendor to provide the Services.

Section 25: NO COLLUSION.

Vendor represents and certifies that (1) Vendor is not barred from contracting with a unit of state or local government as a result of (a) a delinquency in the payment of any tax administered by the Illinois Department of Revenue unless Vendor is contesting, in accordance with the procedures established by the appropriate revenue act, its liability for the tax or the amount of the tax; or (b) a violation of either Section 33E-3 or Section 33E-4 of Article 33E of the Illinois Criminal Code of 1961, 720 ILCS 5/33E-1 et seq.; (2) only persons, firms, or corporations interested in this Agreement as principals have been those disclosed to the Park District prior to the execution of this Agreement; and (3) this Agreement is made by Vendor without collusion with any other person, firm, or corporation. If at any time it shall be found that Vendor during this Agreement, colluded with any other person, firm, or corporation, then Vendor shall be liable to the Park District for all loss or damage that the Park District may suffer, and this Agreement shall, at the Park District's option, be null and void.

Section 26: SEXUAL HARASSMENT POLICY/NON-DISCRIMINATION.

Vendor certifies that it has a written Sexual Harassment Policy in full compliance with 775 ILCS 5/2-105(A)(4). In all hiring or employment by Vendor pursuant to this Agreement, there shall be no discrimination against any employee or applicant for employment because of age, race, gender, creed, national origin, marital status, or the presence of any sensory, mental, or physical handicap, unless based upon a bona fide occupational qualification. Vendor agrees that no person shall be denied or subjected to discrimination in receipt of the benefit of any services or activities made possible by, or resulting from, this Agreement.

Section 27: MISCELLANEOUS PROVISIONS.

- A. Amendments: No modification of this Agreement shall be effective unless in writing dated a date subsequent to the date of this Agreement and signed by an authorized representative of each of the Parties hereto.
- B. Successors and Assigns: The provisions, covenants and conditions in this Agreement shall bind the Parties, their legal heirs, representatives, successors, and assigns.
- C. Remedies Cumulative: Rights under this Agreement are cumulative and nonexclusive of any other remedy at law or in equity.
- D. Severability: If any term or provision of this Agreement is determined by a court of competent jurisdiction to be invalid or unenforceable, the remainder of this Agreement shall not be affected thereby, and each term and provision of this Agreement shall be valid and enforceable to the fullest extent permitted by law.
- E. Waiver: No covenant, term or condition or the breach thereof shall be deemed waived, except by written consent of the Party against whom the waiver is claimed, and any waiver of the breach of any covenant, term or condition shall not be deemed to be a waiver of any preceding or succeeding breach of the same or any other covenant, term or condition. Neither the acceptance by the Park District of any performance by Vendor after the time the same shall have become due nor payment to Vendor for any portion of the Services shall constitute a waiver by the Park District of the breach or default of any covenant, term or condition unless otherwise expressly agreed to by the Park District in writing.

- F. Entire Agreement: This Agreement, along with any exhibits and attachments, constitutes the entire agreement between the Parties with respect to the Services. No verbal agreement or conversation between any officer, agent, associate or employee of the Park District and any officer, agency, employee or associate of Vendor prior to the execution of this Agreement shall affect or modify any of the terms or obligations contained in this Agreement.
- G. Negotiated Agreement: The Parties acknowledge that this is a negotiated agreement, that they have had the opportunity to have this Agreement reviewed by their respective legal counsel, and that the terms and conditions of this Agreement are not to be construed against any Party on the basis of such Party's draftsmanship thereof.
- H. Headings: The various headings used in this Agreement as headings for sections or otherwise are for convenience only and shall not be used in interpreting the text of the section which they appear.
- I. Notices: All notices, demands, requests, exercises and other communications required or permitted to be given by either Party under this Agreement shall be in writing and:
- (a) shall be sent by personal delivery, in which case notice shall be deemed delivered on the date of receipt by the other Party; or
 - (b) shall be sent by facsimile or e-mail if a copy of the writing is also sent by United States Certified Mail, pursuant to subparagraph (d) below, in which case notice shall be deemed delivered on the date and at the time of transmittal by facsimile or e-mail, provided that a transmission report is generated that reflects the accurate transmission date and time of the writing; or
 - (c) shall be sent by a nationally recognized overnight courier, in which event notice shall be deemed delivered one (1) business day after deposit with that courier; or
 - (d) shall be sent by United States Certified Mail, return receipt requested, in which case notice shall be deemed delivered three (3) business days after deposit, postage prepaid, in the United States Mail.

All such notices shall be addressed as follows:

If to the Vendor:

Attn: Jeremy Wills
Advanced Intelligence Engineering
104 E. Roosevelt Road Suite 101
Wheaton, IL 60189
Phone: 630-936-4045
Fax:

If to the Park District:

Attn: Executive Director
Wheaton Park District

102 E. Wesley Street
Wheaton, IL 60187
Phone: 630-510-4955
Fax: 630-665-5880

IN WITNESS WHEREOF, in consideration of the terms, conditions, and covenants contained herein, or attached and incorporated and made a part hereof, the Parties have executed this Agreement by having their representatives affix their signatures below.

Wheaton Park District

By



1/21/2022

Signature

Date

Michael J. Bernard, Executive Director

Printed Name

Title

Advanced Intelligence Engineering

By



01-28-2022

Signature

Date

Jeremy Wins

PRESIDENT

Printed Name

Title



ADVAN-3

OP ID: DG

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

12/30/2021

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Advanced Insurance Partners 1755 S. Naperville Rd. Ste 100 Wheaton, IL 60189 Dirk Glass	630-462-7008	CONTACT NAME: Dirk Glass PHONE (A/C, No, Ext): 630-462-7008 FAX (A/C, No): 630-462-7030 E-MAIL ADDRESS: dglass@aipinsurance.com
INSURED Advanced Intelligence Engineering, LLC 104 E Roosevelt Rd Ste 101 Wheaton, IL 60187		INSURER(S) AFFORDING COVERAGE INSURER A : Travelers Insurance Company INSURER B : Lloyd's of London INSURER C : INSURER D : INSURER E : INSURER F :
		NAIC # 25658 15792

COVERAGES

CERTIFICATE NUMBER:

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSD WVP	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC OTHER:	X	6806H797422142	09/01/2021	09/01/2022	EACH OCCURRENCE \$ 2,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 300,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ 2,000,000 GENERAL AGGREGATE \$ 4,000,000 PRODUCTS - COMP/OP AGG \$ 4,000,000
A	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO OWNED AUTOS ONLY <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY	X	6806H797422142	09/01/2021	09/01/2022	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 5000	X	CUP6H7073312142	09/01/2021	09/01/2022	EACH OCCURRENCE \$ 3,000,000 AGGREGATE \$ 3,000,000
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) <input type="checkbox"/> Y/N If yes, describe under DESCRIPTION OF OPERATIONS below	N/A				PER STATUTE <input type="checkbox"/> OTH-ER <input type="checkbox"/> E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
B	Professional &		W1FED4200401	09/01/2021	09/01/2022	E&O/Cyber \$ 2,000,000
B	Cyber/Data Breach		W1FED4200401	09/01/2021	09/01/2022	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Wheaton Park District, its elected and appointed officials, employees, agents, and volunteers are all additional insureds on the general liability. Travelers gives blanket additional insured, primary and non-contributory, coverage where required by contract

CERTIFICATE HOLDER

CANCELLATION

WHEATPD

Wheaton Park District
1777 S. Blanchard St.
Wheaton, IL 60189

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Wheaton Park District

Request for Proposal

Managed Services - Information Technology Operations

(RFP ID: WPDMS)

July 1, 2021

Table of Contents

1	STATEMENT OF WORK	3
1.1	PURPOSE	3
1.2	GENERAL SCOPE	3
1.3	SUBMISSION PROCESS, DUE DATE AND REQUIRED DOCUMENTS	3
2	GENERAL INFORMATION.....	4
2.1	ORIGINAL RFP DOCUMENT	4
2.2	THE ORGANIZATION	4
2.3	EXISTING TECHNOLOGY ENVIRONMENT	5
2.4	SCHEDULE OF EVENTS	7
3	PROPOSAL PREPARATION INSTRUCTIONS.....	8
3.1	VENDOR'S UNDERSTANDING OF THE RFP	8
3.2	GOOD FAITH STATEMENT	8
3.3	PROPOSAL SUBMISSION	10
3.4	CRITERIA FOR SELECTION	10
3.5	SELECTION AND NOTIFICATION.....	10
4.	REQUIREMENTS.....	13
5.	COST.....	14
6.	ADDITIONAL TERMS & CONDITIONS	15
6.1	CONTRACT DOCUMENTS.....	15
6.2	NON-DISCLOSURE AGREEMENT	15
6.3	COSTS	15
6.4	PAYMENT	15
6.5	INTELLECTUAL PROPERTY.....	15
6.6	INSURANCE REQUIREMENTS	15
6.7	INDEMNIFICATION	18
6.8	RFP RESPONSES.....	18
6.9	GOVERNING LAW.....	18
6.10	NO LIABILITY	18
6.11	ENTIRE RFP	18
6.12	COMPLIANCE WITH LAWS.....	19
7.	VENDOR CERTIFICATION	20
	SCHEDULE "A" NOTICE OF INTENTION.....	22
	ATTACHMENT A – INVENTORY SUMMARY	
	ATTACHMENT B – DETAILS OF TECHNOLOGY COMPONENTS AND A NETWORK DIAGRAM	
	ATTACHMENT C - SAMPLE WPD MANAGED IT SERVICES AGREEMENT	

1 Statement of Work

1.1 Purpose

The purpose of this Request for Proposal (RFP) is to invite prospective vendors to submit proposals to manage the information technology (IT) operations for the Wheaton Park District (the "District", "Park District", "Wheaton Park District" or "WPD").

1.2 General Scope

The intended scope of this RFP, and any agreement resulting from this RFP, shall be for the management of information technology operations for the Wheaton Park District.

1.3 Submission Process, Due Date and Required Documents

All parties submitting proposals must be addressed and delivered to the email address listed below, which is the address to be used for all communication in connection with this project:

rtrainor@wheatonparks.org
ssimpson@wheatonpark.org

Proposals must be received on or before August 2, 2021 at 5 PM (Central) to be considered. Proposals received after this deadline shall not be considered.

Upon review of proposals received in response to this RFP, the Park District will enter into a contract with the vendor that is best qualified based on the criteria set forth in this RFP, is responsible and responsive to requested criteria and which provides the best overall value to the District. The bid cost is not the only criteria for selection.

The District reserves the right to reject any and all proposals, or to accept any portion of the proposal, to waive any formality, technicality or irregularity in any proposal, and to be the sole judge of the value and merit of the proposals offered. Such decisions by the District shall be final.

2 General Information

2.1 Original RFP Document

The Wheaton Park District shall retain the RFP, and all related terms and conditions, exhibits and other attachments, in original form in an archival copy. Any modification of these in the vendor's submission is grounds for immediate disqualification.

2.2 The Organization

The Wheaton Park District was established as a separate municipal body by the citizens of Wheaton in 1921. Land for its first park, Memorial Park, was purchased in 1921, with Southside (now Central) Park acquired in 1922, and Northside Park soon after. Through both acquisition and donation, the district increased its park acres to 94 by 1970. Today the citizens of the district enjoy 52 park sites totaling more than 800 acres.

The Wheaton Park District has one of the finest park systems in the state, and has been recognized many times:

- National Park & Recreation Association with the National Gold Medal for Excellence in Park and Recreation Management (2005, 1996, 1990 and 1984)
- Illinois Park and Recreation Association Outstanding Program Award (2008)
- Illinois Park and Recreation Association's Distinguished Agency Award (1999)
- U.S. Department of Interior Innovation Award (1993) for the Lincoln Marsh Wetlands Project
- Excellence in Financial Reporting certificate by the GFOA every year for 32 years running.
- The Aquatics staff earned the "Gold Award" with a score that exceeds on all three of their safety audits (2019).

The Wheaton Park District operates a wide variety of facilities including:

- Arrowhead Golf Club
- Central Athletic Center
- Clocktower Commons - Mini Golf and Skate Park

- Community Center
- Cosley Zoo
- Lincoln Marsh Natural Area and Teams Course
- Mary Lubko Center
- Northside Family Aquatic Center
- Parks Plus Fitness Center
- Rice Pool and Water Park
- Safety City
- DuPage Historical Museum
- Cosley House
- Parks Service Center
- Prairie office

2.3 Existing Technology Environment

The Wheaton Park District facilities include the following technology components running the key applications listed subsequently. Attachment A provides a current inventory for the Wheaton Park District. The servers listed are currently centralized in one site in Wheaton.

- **Technology Components:**

175 Desktops / Laptops

15 Virtual Machines (3 VM Hosts VMware)

Active Directory environment

Office 365 (email)

Image level and offsite replicated backup and disaster protection system

NAS/ SAN

54 Cisco Network devices

19 Internet Circuits (Voice and Data)

SIP-based cloud phone system

POTS lines throughout Park District facilities

Multi-function printers throughout Park District facilities

Remote access to Park District security camera servers

Network security provided by managed SOC solution

Dark web monitoring (for credentials security)

Anti-phishing/Security awareness training service

NOTE: Attachment A provides a current inventory for the WPD; Attachment B provides additional details for the Technology Components and a Network Diagram.

- **Applications:** For most of the applications that follow, the vendor is expected to support the underlying infrastructure and not necessarily specific functions within the application. Experience with some of the more critical vendor applications is a definite plus (e.g. Vermont Systems RecTrac & Web Trac, Paylocity-application is cloud based but the timeclocks are on a virtual server).

Springbrook Financial Systems – Financial software

Vermont Systems RecTrac – Parks and Recreation Management software

Vermont Systems WebTrac – Online recreation registration software

Paylocity – Payroll service

Digital Dining – Restaurant POS software

FitnessGram – Fitness assessment and reporting program

ZooTriton – A comprehensive database for zoo and wildlife managers

Past Perfect Software – Museum collection management software

Phoenix Software for Advanced Management – Fuel tracking software

Autodesk MapGuide Enterprise – Web-based mapping software for sharing CAD, GIS, and other infrastructure asset information

AutoDesk – AutoCAD Map 3D Esri – ArcEditor (now ArcGIS)

Trimble – Pathfinder Office for the desktop

Trimble – Terrasync for the GPS handheld

Trimble – Total Station (Survey Pro)

Microsoft Office Suite

Miscellaneous Software Applications – Unique to Departments

Security Camera System Control

- HiKVision DVR and camera viewing software
- Arrowhead Golf Club (AGC) – CCTV security system

2.4 Schedule of Events

The following is a tentative schedule for this RFP, but may change in accordance with the Park District's needs or for unforeseen circumstances. Changes will be communicated by email to all vendors who have received this RFP.

Issuance of RFP	July 1, 2021
Notice of Intent to Respond returned	July 14, 2021
Technical Questions/Inquiries due	July 22, 2021
RFP Closes	August 2, 2021
Complete Initial Evaluation	August 20, 2021
Finalist Presentations/Q&A	August 23 – September 3, 2021
Final Award Notification	October 20, 2021
Vendor Fully Operational	December 31, 2021

3 Proposal Preparation Instructions

3.1 Vendor's Understanding of the RFP

In responding to this RFP, the vendor accepts full responsibility to review and understand the RFP in its entirety, and in detail, including making any inquiries to the Wheaton Park District as necessary for clarification and information. Failure to make such review or inquiry shall not excuse the vendor from performance of the duties and obligations imposed under the terms of the contract. Once the award has been made, failure to have read all the conditions, instructions and specifications of this contract shall not be cause to alter the original contract or to request additional compensation.

Further, the Wheaton Park District reserves the right, at its sole discretion, to eliminate from further consideration any proposal the Park District deems to be substantially or materially unresponsive to the requests for information contained herein. Such elimination shall be at no fault, cost, or liability whatsoever to the Wheaton Park District.

3.2 Good Faith Statement

All information provided by the Wheaton Park District in this RFP is offered in good faith. Individual items are subject to change at any time. The Wheaton Park District makes no representations or certifications regarding the accuracy of the information provided in this RFP. The Wheaton Park District is not responsible or liable for any use of the information or for any claims asserted from such information.

Communication

Verbal communication shall not be effective unless formally confirmed via email to **rtrainor@wheatonparks.org**. In no case shall verbal communication govern over written communication.

- 3.2.1 **Vendors' Inquiries.** Applicable terms and conditions herein shall govern communications and inquiries between the Wheaton Park District and vendors as they relate to this RFP. Inquiries, questions, and requests for clarification related to this RFP are to be emailed to **rtrainor@wheatonparks.org** as indicated in the following sections.

3.2.2 **Formal Communications** shall include, but are not limited to:

- Questions concerning this RFP, which must be submitted via email to **rtrainor@wheatonparks.org** and be received no later than July 22, 2021.
- Errors and omissions in this RFP and enhancements. Vendors shall recommend to the Wheaton Park District any discrepancies, errors, or omissions that may exist within this RFP. With respect to this RFP, vendors shall recommend to the Wheaton Park District any enhancements, which might be in the Wheaton Park District's best interests. These must be submitted via email to **rtrainor@wheatonparks.org** and be received no later than July 22, 2021.
- Inquiries about technical interpretations, which must be submitted via email to **rtrainor@wheatonparks.org** and be received no later than July 22, 2021.
- Verbal and/or written presentations and pre-award negotiations under this RFP.
- Addenda to this RFP.

3.2.3 **Addenda:** The Wheaton Park District will make a good-faith effort to provide an email response to each question or request for clarification, interpretation or changes within three (3) business days. All questions, answers, and addenda will be shared with all recipients of this RFP.

The Wheaton Park District will not respond to any questions or requests for clarification that require addenda, if received by the Wheaton Park District after July 22, 2021.

3.3 Proposal Submission

Proposals must be emailed to **rtrainor@wheatonparks.org** no later than 8 AM, CST on August 2, 2021. Submissions must include both this document and the supporting spreadsheet (with all tabs completed). Any additional information submitted by the vendor must be clearly marked with the RFP ID and must be referenced within the base documents above.

2021 Wheaton Park District RFP Managed IT Services – Vendor Response.xlsx

Proposals must be submitted in the format outlined in this RFP. Each proposal will be reviewed for completeness prior to actual evaluation. The Park District reserves the right to eliminate from further consideration any proposal the Park District deems to be substantially or materially unresponsive to the requests for information contained herein.

A proposal may not be modified, withdrawn or canceled by a vendor after the time and date designated for receipt of proposal. A vendor may withdraw or modify a submitted proposal before the time and date designated for receipt by providing a written notice to the party receiving proposals on behalf of the Park District as noted herein.

3.4 Criteria for Selection

The evaluation of each RFP response will be based on its demonstrated competence, compliance, format, and organization. The purpose of this RFP is to identify those vendors that have the interest, capability, and financial strength to supply the Wheaton Park District with managed IT operations support. The selected vendor must have the capability to provide proactive support not just reactive support. They must show a breadth of technical experience to cover all potential situations that they could encounter with the District's current technological environment.

The following spreadsheet must be completed and included in the proposal submission. This information is in the "Criteria for Selection" tab of the spreadsheet.

2021 Wheaton Park District RFP Managed IT Services – Vendor Response.xlsx

3.5 Selection and Notification

The evaluation team members will read and evaluate the proposals and rank the firms accordingly based on the firm's qualifications, personnel, experience, cost,

conformity with the RFP, and other factors. The recommendation of the evaluation team will be subject to approval by the Wheaton Park District Board of Park Commissioners. The District anticipates that the contract will be awarded at the October 20, 2021 Board Meeting.

Vendors determined by the Wheaton Park District to possess the capacity to compete for this contract will be selected to move into the presentation phase of this process. Notification will be sent to these vendors via email. Those vendors not selected for the presentation phase will not be notified.

3.6 Evaluation Criteria

RFP responses will be evaluated to determine the ability of each vendor to provide the required services. WPD will select the firm that best meets the District's needs with price being only one factor that the District will consider to make this determination. The recommendation of the evaluation team will be subject to approval of the Wheaton Park District Board of Commissioners.

The District will award the contract to the vendor based on the following evaluation criteria:

a. Experience and Qualifications

Experience will be judged based on criteria described in Section 3.4. Preference will be given to respondents demonstrating strong capabilities, experience and reputation in projects similar to those described in this RFP and providing authoritative documentation of the respondent's financial condition and stability. Additionally, the experience of key individuals will be an important factor in the District's evaluation of each vendors overall experience.

b. Proposal Preparation and Approach to the Project

Proposals must follow the format described herein and should include a detailed and sound approach to the scope of services required to achieve the District's objectives.

c. Cost of Services

All elements of pricing requested in Section 5 are important.

d. Ability to Effectively Provide the Services

Vendor proposals should illustrate that they can provide a reliable and proven approach to establish and effectively maintain the managed IT services described in this RFP. At a minimum, essential elements of managed IT services provided to WPD should include: timely responses, detailed record keeping, a

user-friendly help-desk including a web portal for District Users, and the ability to proactively fix root causes so that issues are minimized.

e. Comprehensive Training and Transitional Services

Vendor proposals should describe the ability to effectively document and train Park District users on any transitional and ongoing support procedures.

3.7 Award of Contract

Successful vendor will be notified by the District following the October 20, 2021 Wheaton Park District Board of Park Commissioners meeting.

- . The vendor awarded this project shall enter into a contract with the District substantially in the same form as attached to this RFP.
- . A certificate of insurance identifying the District as additional insured is required within 5 business days upon award of project.

3.8 Cancellation of Request for Proposals

The District reserves the right to cancel this request for proposal at any time, to elect not to award the work listed, to reject any or all of the responses, to waive any informality or irregularity in any response received, and is the sole judge of the merits of the respective responses received. While the District intends to award all tasks included in this request for proposal to one vendor, the District also reserves the right to contract any task or portion of this work separately.

4. Requirements

The overall scope for this RFP is the effective provision of information technology support for the Wheaton Park District and the associated hardware, software, and applications in use.

The following spreadsheet must be completed and included in the proposal submission. This information is in the “Requirements” tab of the spreadsheet.

2021 Wheaton Park District RFP Managed IT Services – Vendor Response.xlsx

5. Cost

The following spreadsheet must be completed and included in the proposal submission. This information is in the “Cost” tab of the spreadsheet. (Note: The Wheaton Park District is expecting to implement a 3-year contract with the selected vendor.)

2021 Wheaton Park District RFP Managed IT Services – Vendor Response.xlsx

6. Additional Terms & Conditions

6.1 Contract Documents

The vendor awarded this project shall enter into a contract with the District substantially in the same form as attached to this RFP ([refer to Attachment C](#)) and based on terms and conditions as approved by the District. This RFP, the vendor's proposal, the negotiated contract and any other documents specified by the District shall form the Contract Documents.

6.2 Non-Disclosure Agreement

The Wheaton Park District reserves the right to require any RFP vendor to enter into a non-disclosure agreement.

6.3 Costs

The RFP does not obligate the Wheaton Park District to pay for any costs, of any kind whatsoever that may be incurred by a vendor or any third parties, in connection with the RFP response. All RFP responses and supporting documentation shall become the property of the Wheaton Park District, subject to claims of confidentiality in respect of the RFP response and supporting documentation.

6.4 Payment

Payment shall be made by the District to the vendor upon the District's receipt of an invoice itemizing the services performed for the period covered by the invoice. The vendor will invoice the District on a monthly basis. Payments of all invoices, and any late payment penalties, shall be governed by the Local Government Prompt Payment Act (5 ILCS 505/1 *et seq.*).

6.5 Intellectual Property

The RFP vendor should not use any intellectual property of the Wheaton Park District including, but not limited to, all logos, registered trademarks, or trade names of the Wheaton Park District, at any time without the prior written approval of the Wheaton Park District, as appropriate.

6.6 Insurance Requirements

The successful vendor shall procure, keep in full force and effect, and maintain at its own cost and expense, for the duration of this Agreement, insurance against claims for injuries to persons or damages to property, intellectual property claims, and any

third party intellectual property claims, which may arise from or in connection with the performance of the services hereunder by the vendor, its agents, representatives, employees, or subcontractors. The District shall be named as the certificate holder and identified as an additional insured party on the vendor's Commercial General Liability policy on the Certificate of Insurance.

The vendor shall maintain insurance limits no less than the following:

1. Commercial General and Umbrella Liability Insurance. Vendor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than \$2,000,000 for each occurrence. If such CGL insurance contains a general aggregate limit, it shall apply separately to this project/location. CGL insurance shall be written on Insurance Services Office (ISO) occurrence form CG 00 01 10 93, or a substitute form providing equivalent coverage, and shall cover liability arising from premises, operations, independent contractors, products-completed operations, personal injury and advertising injury, and liability assumed under an insured Agreement (including the tort liability of another assumed in a business Agreement). The District shall be included as an insured under the CGL, using ISO additional insured endorsement CG 20 26 or a substitute providing equivalent coverage, and under the commercial umbrella, if any. This insurance shall apply as primary insurance with respect to any other insurance or self-insurance afforded to the District. Any insurance or self-insurance maintained by the District shall be excess of Company's insurance and shall not contribute with it.

2. Professional Liability Insurance. Vendor shall maintain professional liability and, if necessary, commercial umbrella liability insurance with a limit of not less than \$1,000,000 for each wrongful act arising out of the performance or failure to perform professional services and \$1,000,000 aggregate.

3. Business Auto and Umbrella Liability Insurance. Vendor shall maintain business auto liability and, if necessary, commercial umbrella liability insurance with a limit of not less than \$1,000,000 for each accident. Such insurance shall cover liability arising out of any auto including owned, hired and non-owned autos. Business auto insurance shall be written on Insurance Services Office (ISO) form CA 00 01, CA 00 05, CA 00 12, CA 00 20, or a substitute form providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage equivalent to that provided in the 1990 and later editions of CA 00 01.

4. Workers Compensation Insurance. Company shall maintain workers compensation and employers liability insurance. The commercial umbrella and/or employers liability limits shall not be less than \$1,000,000 each accident for bodily injury by accident or \$1,000,000 each employee for bodily injury by disease.

If District has not been included as an insured under the CGL using ISO additional insured endorsement CG 20 26 under the Commercial General and Umbrella Liability Insurance required in this Contract, Company waives all rights against District and its officers, officials, employees, volunteers and agents for recovery of damages arising out of or incident to this Agreement.

5. General Insurance Provisions

a) Evidence of Insurance

Company shall furnish District with a certificate(s) of insurance and applicable policy endorsement(s), executed by a duly authorized representative of each insurer, showing compliance with the insurance requirements set forth above.

All certificates shall provide for 30 days' written notice to District prior to the cancellation or material change of any insurance referred to therein. Written notice to District shall be by certified mail, return receipt requested.

Failure of District to demand such certificate, endorsement or other evidence of full compliance with these insurance requirements or failure of District to identify a deficiency from evidence that is provided shall not be construed as a waiver of Company's obligation to maintain such insurance.

District shall have the right, but not the obligation, of prohibiting Company from entering the premises until such certificates or other evidence that insurance has been placed in complete compliance with these requirements is received and approved by District.

Failure to maintain the required insurance may result in termination of this Contract at District's option.

Company shall provide certified copies of all insurance policies required above within 10 days of Districts' written request for said copies.

b) Acceptability of Insurers

For insurance companies which obtain a rating from A.M. Best, that rating should

be no less than A VII using the most recent edition of the A.M. Best's Key Rating Guide. If the Best's rating is less than A VII or a Best's rating is not obtained, the District has the right to reject insurance written by an insurer it deems unacceptable.

c) Deductibles and Self-Insured Retentions

Any deductibles or self-insured retentions must be declared to the District. At the option of the District, the Company may be asked to eliminate such deductibles or self-insured retentions as respects the District, its officers, officials, employees, volunteers and agents or required to procure a bond guaranteeing payment of losses and other related costs including but not limited to investigations, claim administration and defense expenses.

d) Subcontractors

Company shall cause each subcontractor employed by Company to purchase and maintain insurance of the type specified above. When requested by the District, Company shall furnish copies of certificates of insurance evidencing coverage for each subcontractor.

6. Cyber Risk Insurance. Subject to the limit of at least \$1,000,000 per claim, minimum of at least \$2,000,000 in the aggregate, to be maintained for the term of the MSA and three years following its termination, to respond to privacy and network security liability claims including, but not limited to the following, and arising directly or indirectly from IT Vendor's failure to carry out its obligations under the MSA, or the negligent or intentional wrongful act, error or omission of IT Vendor, its employees or agents, or third parties not associated with Customer to whom IT Vendor has given access to the data center premises or systems:

- a) Liability arising from theft, dissemination, and/or use of Customer confidential information, including, but not limited to, bank, credit card account, and personally identifiable information such as name, address, social security numbers, etc., regardless of how the information is stored or transmitted.
- b) Network security liability arising from (i) the unauthorized access to, use of, or tampering with computer systems, including hacker attacks; or (ii) the inability of an authorized third party to gain access to supplier systems and/or Customer data, including denial of service, unless caused by a mechanical or electrical failure or acts of God.
- c) Liability arising from the introduction of a computer virus into, or otherwise causing damage to, Customer's or third person's computer, computer system, network, or similar computer-related property and the data, software, and programs thereon.

- d) Crisis-management expenses (i.e., notification, public relations, reputation damage, forensics, etc.) for a data breach.

The above policies shall provide a waiver of subrogation. Customer its elected and appointed officials, officers , employees agents and volunteers shall be included as additional insured with respect to liability arising out of the goods, services and activities performed by or on behalf of IT Vendor.

Professional Liability for IT Technology, including Cyber Risk (Claims-Made):
\$1,000,000 each claim/loss \$2,000,000 aggregate for contracts under \$500,000. (For contracts over \$500,000, \$5,000,000 each claim/loss \$5,000,000 aggregate

The policy shall cover professional misconduct or lack of ordinary skill for persons providing the services to be provided by or on behalf of IT Vendor under the MSA.

IT Vendor warrants that any retroactive date under the policy shall precede the effective date of the MSA; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of three (3) years beginning on the last day of the MSA term. The insurance should provide coverage for the same risks identified above for cyber risk insurance.

IT Vendor does not provide insurance to cover losses by the Customer at the IT Vendor facility, other than as provided above.

IT Vendor provides insurance for its own losses. This includes insurance to cover day-to-day risks and long-term business continuity.

6.7 Indemnification.

To the fullest extent permitted by law, the Company shall indemnify and hold harmless the District and its officers, officials, employees, volunteers and agents from and against all claims, damages, losses and expenses, including but not limited to legal fees (attorney's and paralegals' fees and court costs), arising out of or resulting from the Company's activities, provided that any such claim, damage, loss or expense (i) is attributable to bodily injury, sickness, disease or death, or injury to or destruction of tangible property, and (ii) is caused in whole or in part by any negligent or wrongful act or omission of the Company, any Subcontractor, anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable, except to the extent caused in part by a party indemnified hereunder. Such obligation shall not be construed to negate, abridge, or otherwise reduce any other right or obligation of indemnity which would otherwise exist as to any party or person described in this Paragraph. Company shall similarly protect, indemnify and hold and save harmless the District, its officers, officials, employees, volunteers and agents against and from any and all claims, costs, causes, actions and expenses including but not limited to legal fees, incurred by reason of Company's breach of any of its obligations under, or Company's default of, any provision of the Contract.

6.8 RFP Responses

All accepted RFP responses shall become the property of the Wheaton Park District and will not be returned.

6.9 Governing Law

This RFP vendor and the RFP response shall be governed by the laws of the state of Illinois.

6.10 No Liability

The Wheaton Park District shall not be liable to any vendor, person, or entity for any losses, expenses, costs, claims, or damages of any kind:

- Arising out of, by reason of, or attributable to, the vendor responding to this RFP; or
- As a result of the use of any information, error, or omission contained in this RFP document or provided during the RFP process.

6.11 Entire RFP

This RFP, any addenda to it, and any attached schedules, constitute the entire RFP.

The proposal of the vendor awarded the contract for this RFP will be incorporated by reference into the contract the Park District enters into with the successful bidder.

6.12 Compliance with Laws

The vendor and any contractors or subcontractors hired by the vendor shall comply with all applicable federal and state laws and local ordinances and regulations in the performance of the work.

7. Vendor Certification

This certification attests to the vendor's awareness and agreement to the content of this RFP and all accompanying calendar schedules and provisions contained herein.

The vendor must ensure that the following certificate is duly completed and correctly executed by an authorized officer of its company.

This proposal is submitted in response to RFP for WPDMS, dated July 1, 2021, issued by the Wheaton Park District. The undersigned is a duly authorized officer, hereby certifies that:

(RFP Vendor Name)

agrees to be bound by the content of this proposal and agrees to comply with the terms, conditions, and provisions of the referenced RFP and any addenda thereto in the event of an award. Exceptions are to be noted as stated in the RFP. The proposal shall remain in effect for a period of 120 calendar days as of July 1, 2021.

The undersigned further certify that their firm (check one):

- ☐ IS
☐ IS NOT

currently debarred, suspended, or proposed for debarment by any federal entity. The undersigned agree to notify the Wheaton Park District of any change in this status, should one occur, until such time as an award has been made under this procurement action.

Person[s] authorized to negotiate on behalf of this firm for purposes of this RFP are:

Name: _____

Title: _____

Signature: _____

Date: _____

Name: _____

Title: _____

Signature: _____

Date: _____

Signature of Authorized Officer:

Name: _____

Title: _____

Signature: _____

Date: _____

Schedule "A" Notice of Intention

RFP ID: WPDMS

NOTICE OF INTENTION

REQUEST FOR PROPOSAL

From:

[VENDOR ORGANIZATION NAME]

[AUTHORIZED REPRESENTATIVE]

[TELEPHONE NO.]

[FAX NO.]

[EMAIL]

Please state your intention with regard to the Request for Proposal [RFP ID] by selecting one of the following:

[] Intends to respond to the Wheaton Park District Request for Proposal

[] Does not intend to respond to the Wheaton Park District Request for Proposal

TO:

rtrainor@wheatonparks.org

Wheaton Park District

IT Support RFP Timeline for 2021

Update RFP
documentLegal
review
of RFP

Circulate RFP

Review
ResponsesInterview
FinalistsSelect
FinalistPrepare board
recommendation

Complete by: *Description of item to be completed by date indicated:*

<input type="checkbox"/>	5/28/2021	Mike to email RFP document to nonparticipating consultant for feedback
<input type="checkbox"/>	Week of 6/14/2021	Send RFP document to Legal for review
<input type="checkbox"/>	7/1/2021	Email out RFP document
<input type="checkbox"/>	7/14/2021	Notice of intent to respond due back
<input type="checkbox"/>	7/22/2021	Technical Questions/Inquiries due
<input type="checkbox"/>	8 AM CST, 8/2/2021	Responses due back (electronically) to the RFP document
<input type="checkbox"/>	8/2/2021 – 8/20/2021	Responses reviewed and finalists selected for in person interview
<input type="checkbox"/>	8/23/2021 – 9/3/2021	Interviews with finalists scheduled and conducted in these two weeks
<input type="checkbox"/>	9/7/2021 – 9/17/2021	Finalist selected and board recommendation prepared
<input type="checkbox"/>	9/30/2021	Final recommendation to Mike to go out in the Finance Committee package
<input type="checkbox"/>	10/6/2021	Committee review of recommendation
<input type="checkbox"/>	10/20/2021	Board meeting with this item on the agenda
<input type="checkbox"/>	12/31/2021	Winning vendor fully operational

Exhibit B



WHEATON PARK DISTRICT

RFP:
Information
Technology
Services

AIE WPDMS RFP Response Document
(supporting document 2 of 4)

Donna Siciliano

From: Jeremy Wills <jwills@aie195.com>
Sent: Sunday, August 1, 2021 5:44 PM
To: Sandra Simpson
Subject: AIE Response to the WPD Managed Services 2021 RFP
Attachments: AIE WPDMS RFP Response Document (supporting document 2 of 4).pdf; AIE Technical Project Staff Resumes WPDMS Response (supporting document 3 of 4).pdf; WPDMS AIE Accomplishments (supporting document 4 of 4).pdf; WPD RFP Managed Services 2021 FINAL.docx; 2021 Wheaton Park District RFP Managed IT Services - FINAL.xlsx; WPDMS RFP - Sample AIE Managed IT Services Agreement (supporting document 1 of 4).pdf
Signed By: jwills@aie195.com
Importance: High

Hello Sandra,

Thank you for the opportunity to provide a response to the WPD Managed Services RFP. We hope that our past six years of service—along with our included response—demonstrate our competency and commitment to excellence as we joyfully serve WPD's IT support needs. The following documents are attached as part of our response:

- WPDMS RFP - Sample AIE Managed IT Services Agreement (supporting document 1 of 4)
- AIE WPDMS RFP Response Document (supporting document 2 of 4)
- AIE Technical Project Staff Resumes WPDMS Response (supporting document 3 of 4)
- WPDMS AIE Accomplishments (supporting document 4 of 4)
- 2021 Wheaton Park District RFP Managed IT Services – FINAL (base document)
- WPD RFP Managed Services 2021 FINAL (base document)

We look forward to hearing back from the WPD team with good news of a continued future partnership together!

Sincerely,

Jeremy Wills
Advanced Intelligence Engineering
Office: 630-936-4045 x102 | Fax: 815-346-5342
Email: jwills@aie195.com



*"transforming technology from an overhead
expense to a driver of profit and savings"*

Introduction

The Wheaton Park District boasts a complex, multi-site environment with support requirements ranging from a virtualized group of Windows-based servers, network backbone management, end-user help desk support, vCIO and budgetary guidance, as well as managed security. WPD requires an IT company capable of providing for each of these aspects, while at the same time delivering responsive customer service for the employees and vendors associated with the organization.

The Wheaton Park District continues to strategically invest in their IT infrastructure. Three host servers house 15 virtual machines running in an Active Directory environment, Office 365, Cisco/Meraki network devices, image-level backup and disaster recovery solutions, a SAN/NAS, numerous voice and data circuits, a security camera system, multi-function printers, POTS lines, and numerous security services in-tact. WPD seeks an IT provider capable of supporting the existing environment, with the vision and experience to provide trusted counsel and project assistance as WPD continues to advance with their IT investments.

It is AIE's aim in this proposal to come alongside the Wheaton Park District, serving as trusted advisors in order to move the WPD network forward while maintaining a stable infrastructure inside their current environment.

AIE is uniquely qualified to serve WPD's needs for the following reasons:

- **Competence.** AIE's staff has broad experience in the IT space. Our staff has worked with Fortune 500 companies and government organizations as well as small businesses. We understand how to support and direct the IT function of a large organization, while bearing in mind the budgetary requirements of the organization, and in particular, a government entity.
- **Compassion.** AIE chooses our hires carefully, selecting staff that are not only qualified IT professionals, but demonstrate a high level of integrity, care and concern for their communities. We find this compassion translates well into serving our clients' needs on a daily basis. Client feedback often includes reports that our staff goes above and beyond in support of their IT and their mission.
- **Communication.** AIE understands that our clients will only be as happy with their IT support as they are with our communication. As a result, we have invested heavily in tools to aid in the communication process, including enterprise-level ticketing software and monitoring tools. These tools enable us to proactively communicate throughout all projects, onsite service calls, and remote support work.

Table of Contents

1	Foundational Criteria	1
1.1	Executive Summary.....	1
1.2	Corporate Capability	1
1.3	Corporate Experience	2
1.4	Individual Experience	3
1.5	Financial Stability	5
1.6	Lawsuits.....	5
1.7	Community Involvement	5
2	Technical Experience and Approach	6
2.1	Network Administrative Services.....	6
2.2	Server & Cloud Services Administration Services	7
2.3	Desktop Administration Services	9
2.4	Telecommunications Support	10
3	Help Desk Support Capabilities	12
3.1	Project and Service Delivery Platform	12
4	Client Portal.....	13
5	Support Hours	14
5.1	Business Hours (7:30am – 5:30pm, M-F)	14
5.2	After Hours, Weekends, and Holidays	15
6	Remote Support Tools	15
7	Onsite Support	15
8	Proactive Monitoring Tools.....	16
8.1	Network Monitoring Tools.....	16
9	System Documentation.....	17
9.1	Password Documentation	17
10	Cross Training to Minimize Risk	17
11	Consistent Communication.....	18
11.1	Day-to-Day Communication.....	18
11.2	Management Team.....	18
11.3	Account Reviews	19
12	Troubleshooting / Vendor Management.....	19

12.1	Overview of Service Management Workflow	19
12.2	Service Level Agreements / Escalation Thresholds.....	20
13	Proactive Support	20
13.1	Vendor Support Maintenance	21
13.2	Updates and New Functionality.....	21
14	Strategic Consulting and Budgeting.....	21
15	Equipment Disposal	22
16	Detailed Record Keeping.....	23
17	Onboarding Methodology.....	23
17.1	Approach.....	23
17.2	Timeframe	24
18	Pricing.....	25
18.1	Fixed Monthly Price	25
18.2	Other Monthly Services and Charges.....	25
18.3	Other Fees.....	26

1 FOUNDATIONAL CRITERIA

1.1 EXECUTIVE SUMMARY

Advanced Intelligence Engineering is a Wheaton-based IT consulting firm, dedicated to filling the IT support needs of small and mid-sized businesses and organizations in the Chicagoland area. Jeremy Wills, AIE principal, is a longtime resident of Wheaton. AIE was organized as an LLC in 2007, and has been providing full-service outsourced IT support since that time. Throughout our tenure, AIE has experienced consistently healthy growth, due to our competency, flexibility and experience. Revenues for 2020 were approximately \$1,800,000; we have a current staff of eleven employees.



AIE serves for-profit, non-profit and government accounts, primarily with organizations that have between 10-200 computers. Clients choose to use AIE services over our competition for many reasons. The main reason is our ability to cultivate an intimate relationship with our clients while providing experienced, educated and certified skill-sets to meet advanced corporate requirements. AIE's local Wheaton presence makes us uniquely suited for the Wheaton Park District, as does our focus and experience with organizations of similar size and demands.

1.2 CORPORATE CAPABILITY

The technological landscape changes quickly. To remain competitive, you need expert resources to make intelligent business decisions regarding your IT infrastructure, while keeping change under control for the stability of the organization. At AIE, we go beyond technology for technology's sake and provide true rationale for the use of any current and future IT investments. Our focus is providing managed IT services to small and midsized businesses, including network management, server administration, desktop support, and third-party vendor support. Additionally, AIE provides project work for upgrades and new deployments in all these areas. AIE also offers structured cabling services for clients requiring

data cabling work, wireless infrastructure deployments, hosted cloud solutions, VoIP phone services, and vCIO business consulting.

AIE maintains strong vendor relationships, and is a partner and reseller for Dell, Microsoft, HP, Lenovo, Intuit, Adobe, Cisco, Meraki, and many more. We work with major IT distributors such as Ingram Micro, Synnex, Tech Data and D&H to bring our clients competitive prices on hardware and software. AIE traditionally has taken a vendor-neutral approach while consulting with clients in order to bring the best solutions to the challenge without the conflicting sales motives that leave clients wondering whose best interests are being served. Non-profit and government clients typically receive special discounts on their hardware and software needs.

1.3 CORPORATE EXPERIENCE

Over the years, we have serviced a variety of accounts, many of which share the community-oriented mindset of the Wheaton Park District. We currently support **Memorial Park District**, a park district in Bellwood; **Hyde Park Neighborhood Club**, an after-school program in Chicago focused on the needs of the underprivileged; **Carpenter Training Center**, a non-profit focused on training union carpenters; **Thomas Interiors**, a provider of office furnishings for the modern workspace; and **Roda Specialty Steel**, a national supplier of steel bar and products. With this rich experience in IT services for similarly sized companies, as well as non-profits and government organizations alike, AIE is well equipped to serve the needs of WPD.

AIE recommends the following clients to serve as references for this proposal:

Memorial Park District (Bellwood, IL)

Mark Flores, Facilities Manager / 708-547-5400, ext. 1003 / mflores@mempark.org



AIE has been providing managed IT services to Memorial Park District since 2012. AIE was brought into this account in order to upgrade their core server infrastructure, while providing ongoing support for their RecTrac software and their multi-site network connections, and end-user support. AIE performed a migration of the RecTrac sever from on-premise to the Azure cloud environment.

Hyde Park Neighborhood Club (Chicago, IL)

Angela Habr, Executive Director / 773-643-4062 / ahabr@hpncclub.org



AIE has been providing fully outsourced IT services for Hyde Park Neighborhood since 2012. HPNC is a non-profit organization providing after-school programs in downtown Chicago, and relies heavily on donations and government funding. AIE has helped HPNC go through two iterations of their IT infrastructure to continue to meet their business needs. Most recently, AIE moved the infrastructure from an on-premise server to an Office 365 cloud environment, including Teams, SharePoint and OneDrive.

Carpenter Training Center (Elk Grove Village, IL)

Craig Triplett / 847-640-7373 / ctriplett@chicap.org



AIE began serving the needs of Carpenter Training Center in 2017. A multi-location organization, AIE has helped to upgrade and consolidate the server and network infrastructure, allowing employees in non-headquartered locations the means of accessing systems that they were once unable to access. Additionally, AIE has extensively built out and their wireless local area network to accommodate wireless coverage for their large training facility.

Roda Specialty Steel (Buffalo Grove, IL)

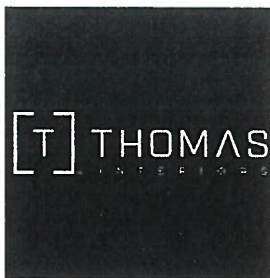
Ann-Marie Stupops, Executive Assistant / 847-279-0228 / annmarie.s@rodaspecialtysteel.com



AIE and Roda have been working together since 2016. Roda is a nation-wide, stainless steel distributor with a presence in several cities around the country. Roda was one of AIE's early adopters of enhanced security solutions, allowing AIE to implement our full security stack into their organization.

Thomas Interiors (Bloomington, IL)

Matt Hills, Vice President of Operations / 312-581-7910 / matth@thomasinteriors.com



AIE began supporting Thomas Interiors in 2019. AIE has executed on numerous projects to help improve the core infrastructure of Thomas Interiors, including installing a new VMware host server, completing an IT rack cleanup, upgrading their key AutoCAD software, and deploying key security services to further harden their IT network.

1.4 INDIVIDUAL EXPERIENCE

Our team of dedicated staff possesses technical IT experience along with creativity and innovation. AIE staff engineers have worked with small business IT as well as within the Fortune 500 and top-tier consultancies. Our engineers have a variety of strengths and backgrounds, combining to make us the company we are today. We choose our hires with careful consideration as we seek to provide our clients quality customer service and technological support.

Our team has earned the following certifications and degrees:

- BA in Business Administration and Change Management
- BS in Computer Science
- BA in Engineering
- BA in Telecommunications
- AAS in Cisco Networking
- AAS Personal Computer Technical Specialist
- Certified Wireless Technology Specialist (CWTS)
- Certified Cisco Networking Associate (CCNA)
- CompTIA A+ Certification
- CompTIA Network+ Certification
- CompTIA Server+ Certification
- Datto Certified Deployment Specialist
- Microsoft Certified Azure Administrator Associate
- Microsoft Certified Security Fundamentals
- Microsoft Certified Systems Associate (MCSA)
- Microsoft Certified Technology Specialist (MCTS)

AIE's technical department is comprised of two teams:

- **Professional Services** – A team of 2 engineers focusing on solutions architecting and special projects
- **Support Services** – A team of 4 technicians who provide service desk support and assistance on projects

Our technical support staff supporting WPD systems include:

Mark Bartlebaugh (Professional Services): Solutions Architect, 20+ years IT experience in multiple technical roles at companies ranging from Fortune 100 to nonprofit and SMB.

Bob Ewoldt (Professional Services): Systems Engineer, 12+ years' IT Support and Engineering (Microsoft, Cisco, VMWare).

Kyle Murphy (Support Services): 7+ years administration of Microsoft and MacOS hardware and software, network support, and Microsoft 365 cloud administration.

Sam Jacob (Support Services): 6+ years Microsoft desktop and server support, firewall management, and mobile device management of Apple and Chrome OS devices.

Daniel Matthews (Support Services): Microsoft desktop support and hardware repair, database administration.

Stephen Schroeder (Support Services): Microsoft and Linux desktop and server support, network engineering and support.

AIE places a high value on the importance of hiring experienced administrative staff. Our operational staff supporting WPD administratively include:

Jeremy Wills: President, Account Manager, 20 + years' experience in business development, operations management, and technology consulting.

Geoff Pearson: Service Delivery Manager, 15 years' experience in IT including desktop, server and network administration, IP telephony support, IT project, account, and service management.

Full resumes are attached for technical personnel listed above who will be key players in projects delivered for WPD should AIE become the successful candidate.

1.5 FINANCIAL STABILITY

With 14 years in business, AIE has a proven track record of financial stability, including the following financial numbers: Total revenues in 2020 were \$1,795,097 with over 60% of the revenue coming in the form of recurring management fees. AIE's target gross revenues for the next twelve months are estimated between \$1.8MM to \$2MM. AIE is a debt-free company.

1.6 LAWSUITS

AIE is not, nor ever has been, involved in any lawsuits, pending or otherwise. AIE has never defaulted on a managed services project or contract.

1.7 COMMUNITY INVOLVEMENT

AIE values community involvement. Both corporately and individually, AIE and its employees make it a priority to invest back into their community.

Corporately, AIE has contributed both financially and through other means to various charities, including a number of our clients:

- Financial contributions to Wheaton Park District (Wheaton, IL)
- Financial contributions to Hyde Park Neighborhood Club (Chicago, IL)
- Financial contributions to Naomi's House (West Chicago, IL)
- Sponsoring and participating in Cosley Zoo Golf Outing (Wheaton, IL)
- Sponsoring staff attendance at Hyde Park Neighborhood Club fundraising gala (Chicago, IL)
- Donating IT equipment to Deaf Video Communications (Carol Stream, IL)

AIE staff are heavily involved in their communities. Our staff's community services include:

- Participating in the Cosley Zoo 5K (Wheaton, IL)
- Providing meals for those in need through in-church ministry (Wheaton, IL)
- Coaching for a local Serve City Volleyball Club (Wheaton, IL)
- Coaching hockey for a local club team (Glenview, IL)
- Active board member while donating money, clothing and time to Dream Foundation, a program to help subsidize the physical needs of low-income students at Whittier Elementary (Wheaton, IL)
- Packing food for Feed My Starving Children (Schaumburg, IL)
- Volunteering time for Lurie Children's Hospital in a variety of ways (Chicago, IL)
- Serving in the local church on the setup team (West Chicago, IL)

- Serving in the local church children's ministry team (West Chicago, IL)
- Serving in the local church worship team (Warrenville, IL and Villa Park, IL)
- Serving in the local church special needs program (Warrenville, IL)
- Serving in the local church A/V team (Warrenville, IL)

2 TECHNICAL EXPERIENCE AND APPROACH

After careful review of the RFP and requirements, AIE has determined our company possesses the qualifications and experience necessary to provide such support.

Should AIE be selected as the vendor in the course of this RFP, AIE will provide IT technical expertise, system monitoring and support, and will recommend hardware and software purchases as needed to meet corporate IT objectives. AIE will also provide security-related recommendations in the interested of hardening the WPD environment against today's cybersecurity threats, including the recommendation of third-party security specialists when needed. Furthermore, AIE will also provide vCIO service on an ongoing basis to provide technical guidance and leadership tailored to the Park District's specific needs and long-term business strategy.

2.1 NETWORK ADMINISTRATIVE SERVICES

2.1.1 Wheaton Park District Requirements

Wheaton Park District requires the selected vendor to provide support for the entire WPD network environment at locations throughout the Park District. This environment includes all network infrastructure devices (such as switches, routers, firewalls and wireless access points), the SIP cloud-based phone system, all ISP links to Park District facilities and the vendor-owned infrastructure used as gateway devices at Park District facilities, analog POTS lines (to be supported in conjunction with vendor support), and oversight of all pertinent security services in the network. This support shall include:

- Regular analysis, routine configuration changes, and installation of patches and updates
- Alerting designated WPD personnel in the event of failure
- Proactive monitoring of network equipment including bandwidth utilization and other performance indicators
- Management and storage of network configuration information
- Network performance and capacity management services
- Network troubleshooting
- Proactive monitoring for intrusion into WPD firewalls
- Maintenance of documentation and procedures

2.1.2 AIE Solution

Should AIE be the selected vendor, AIE will meet these needs through the following services.

2.1.2.1 24x7x365 Remote Monitoring & Automated Reporting

AIE will use Auvik (an industry-respected monitoring tool) and Cisco's Meraki portal for monitoring and management WPD network equipment, including firewalls, routers, switches, and wireless access points. The WPD network will be monitored 24x7x365, and automated alerts will be sent to AIE's service

desk for review and response. Additionally, security-related alerts from RocketCyber with regard to the firewalls will also be sent to the AIE service desk for review and remediation as needed.

2.1.2.2 Regular Maintenance

AIE will manage the WPD network equipment on an ongoing basis. This will include review of router, switch and firewall logs, and troubleshooting of problems, and performance management. AIE will aid WPD in purchasing necessary licensing and hardware for all network infrastructure and will apply needed patches (security-related and otherwise) for all network equipment on an ongoing basis.

2.1.2.3 Diagrams & Network Documentation

AIE will maintain diagrams of the networks at each facility using Auvik, which automatically discovers devices connected to the network and builds a dynamic and interactive diagram which can be exported to a PDF file on demand. In addition, AIE will maintain detailed configuration and network policy information using the Cisco Meraki portal and Auvik (used for non-Meraki devices). In conjunction with WPD staff, AIE will maintain a knowledge of WPD network policies and offer recommendations for best practice improvements. AIE will manage all passwords in a securely encrypted location, along with custom documentation, policy documents, and any supplemental information regarding manufacturer service and maintenance contracts.

2.1.2.4 WAN, WLAN, LAN Management

AIE utilizes Auvik and Meraki to gather information and status on all devices network-wide that are critical to the infrastructure. This information allows us to take rapid action to remediate network connectivity issues when they arise, and to provide early insight into developing problems.

2.2 SERVER & CLOUD SERVICES ADMINISTRATION SERVICES

2.2.1 Wheaton Park District Requirements

Wheaton Park District has 3 physical servers and 14 virtual servers currently in use, running a mixture of Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019. The e-mail service used by the Park District is Microsoft 365, and adoption of Microsoft 365 Apps for Enterprise is increasing.

The following applications are hosted on either on-premise servers or cloud server solutions:

- Active Directory (hosted on Windows Server 2012 R2 and 2019)
- Microsoft 365-hosted e-mail (165 licensed mailboxes)
- Springbrook Financial Systems
- Vermont Systems RecTrac
- Digital Dining
- Paylocity
- FitnessGram
- ZooTriton
- Past Perfect Software
- Phoenix Software for Advanced Management (Fuel tracking)
- AutoDesk – AutoCAD Map 3D Esri – ArcGIS
- Trimble (Pathfinder Office, Terrasync, Total Station)

- Microsoft Office
- HIKVision NVR Software (administered by Imperial)
- CMS CCTV Security System (AGC security camera system)

Wheaton Park District requires the selected vendor to manage WPD servers and cloud environment, including system monitoring, break-fix troubleshooting, backup, and upgrades as needed to the servers, both in the data center and at satellite locations. This administration shall include:

- Ensure scheduled preventative maintenance for equipment is properly and promptly performed
- Maintain the maintenance records on equipment
- Develop operations, administrative, and quality assurance back-up plans and procedural documentation
- Setup new users and edit or remove existing users on servers
- Server performance and capacity management services
- Configuration management, including changes
- Upgrading and patching of servers with product enhancements and security patches, etc.
- Coordinate repair and maintenance work with contracted repair vendors and ensure repairs are conducted in a timely fashion
- Monitor server performance and capacity to recommend adjustments and upgrades as necessary
- Notify designated WPD personnel in the event of failure
- Provide 24/7 on-call support to keep server infrastructure functioning continuously
- Provide security services to detect activity of threat actors within the server infrastructure

2.2.2 AIE Solution

AIE will meet these needs through the following services.

2.2.2.1 24x7x365 Remote Monitoring & Automated Reporting

AIE will install our Remote Monitoring & Management (RMM) agents on all Windows servers. All servers will be monitored 24x7x365, and real-time alerts will be sent to AIE's service desk for rapid evaluation and remediation during business hours, and to the designated technician on call outside of regular business hours. AIE will notify designated WPD staff of steps needed to remediate failures and potentially business-impacting issues. Monitoring will include event logs, service availability, drive space, printer queue availability, and backup success. Performance data from all servers will be available on demand or on a schedule and can be shared with designated Park District personnel upon request.

2.2.2.2 Regular Maintenance and Upgrades

AIE will provide regularly scheduled maintenance for each server on a monthly basis. This maintenance includes the remote patch management and log file maintenance provided for covered servers, along with automated restart of updated servers during off-peak maintenance windows approved by the Park District. Each virtual server is considered a separate server for maintenance purposes. (Server operating system or hardware upgrades are considered separate projects, and are outside of the scope of this proposal.)

2.2.2.3 Remote Support

AIE will provide phone and remote take-control support for server-related issues, including user account administration and file server sharing administration needs. This support will also include those issues with server-based applications, such as RecTrac and AutoCAD. AIE will provide phone and remote support for WPD staff, to ensure that proper function of these applications is restored, and will liaison with vendor support personnel if needed in order to accomplish this.

2.2.2.4 Backup Management

AIE will monitor the success of data backup through the Datto Siris appliances to confirm consistent and successful backups, and to confirm that automatic testing of the backups is operating successfully. As needed, AIE will assist in file restores for individual users.

2.2.2.5 Security Services

As part of server management for the Wheaton Park district AIE will monitor the servers for illegitimate activity using RocketCyber. This will provide visibility into the activities of unauthorized threat actors who have gained access to the server infrastructure and will notify AIE if malicious activity is detected. This will also allow for rapid isolation of an infected server to protect the remainder of the environment from compromise.

2.3 DESKTOP ADMINISTRATION SERVICES

2.3.1 Wheaton Park District Requirements

Wheaton Park District requires the selected vendor to manage the endpoint devices on their network. This administration shall include:

- Installing PCs, laptops, PDAs, printers, peripherals and office automation software
- Diagnosing and correcting desktop application problems
- Configuring laptops and desktops for standard applications
- Identifying and correcting end-user hardware problems
- Performing advanced troubleshooting
- Assist in the development of software/hardware policies and procedures as well as provide or recommend enterprise-wide endpoint protection for all desktops, laptops and servers
- Provide security services to detect activity of threat actors throughout the WPD workstations

2.3.2 AIE Solution

AIE will meet these needs through the following services.

2.3.2.1 24x7x365 Workstation Monitoring & Automated Reporting

AIE will install our Remote Monitoring & Management (RMM) agents on each WPD workstation, including those used as spares. All workstations will be monitored 24x7x365 by means of automated alerting and real-time information in the RMM portal's dashboards. Workstation performance reports will be available on demand or on a schedule and can be delivered to designated Wheaton Park District personnel upon request.

2.3.2.2 Regular Maintenance and Upgrades

AIE will provide remote patch management and optimization for covered workstations. As part of AIE's project engagements, AIE will work with WPD to create a PC replacement plan in order to upgrade computers that are end of life, following a four year rotation for each device.

2.3.2.3 Microsoft Application Support

AIE will provide support for WPD staff using Microsoft Applications on a covered workstation, including Microsoft 365 applications. AIE will also provide regular patch management for Microsoft applications on all covered workstations.

2.3.2.4 Other Application Support

AIE understands that WPD uses a variety of specialized applications for administration, community development, finance, police, and public works. AIE will provide support for WPD staff to ensure these applications are functioning as designed and will liaison with vendor support as necessary to troubleshoot problems and restore functionality.

2.3.2.5 Security Management

AIE will manage that antivirus as part of the 24X7X365 monitoring, and AIE's managed antivirus solution from BitDefender will be installed on all workstations along with the RMM software. If a virus is caught and quarantined, AIE will also use a second-opinion scanner to verify all traces have been removed, in compliance with industry standard best practice.

AIE will also monitor the workstations for illegitimate activity using RocketCyber. This will provide visibility into the activities of unauthorized threat actors who have gained access to any workstations and will notify AIE if malicious activity is detected. This will also allow for rapid isolation of an infected workstation to protect the remainder of the environment from compromise.

2.3.2.6 Procurement Assistance

AIE maintains relationships with several major technology distributors, including CDW, Synnex, D&H, and Ingram Micro, and can also source hardware through Amazon and Newegg. Most of our vendors have Chicago warehouses, often allowing for same or next day procurement of replacement parts. AIE will assist WPD staff in determining what purchases are needed, and will send quotes to the appropriate WPD contact for easy online approval of orders.

2.4 TELECOMMUNICATIONS SUPPORT

2.4.1 Wheaton Park District Requirements

Wheaton Park District requires the selected vendor to administrate all telecommunications systems. This administration shall include:

- Telephony move/add/changes on the existing SIP-trunked VOIP system
- Assistance with cellular/cellular data devices to end users

2.4.2 AIE Solution

Should AIE be the selected vendor, AIE will meet these needs through the following services.

2.4.2.1 Moves/Adds/Changes to Phone System

AIE will administrate all necessary moves/adds/changes for VoIP telephones throughout the network as requested by WPD staff. Further, AIE will provide support to verify that they are communicating properly through the network infrastructure and will provide liaison with Inteliquent technical support staff to isolate and correct issues.

2.4.2.2 Assistance with End-User Devices

AIE will provide support for email and wireless connectivity for WPD employees on authorized devices.

3 HELP DESK SUPPORT CAPABILITIES

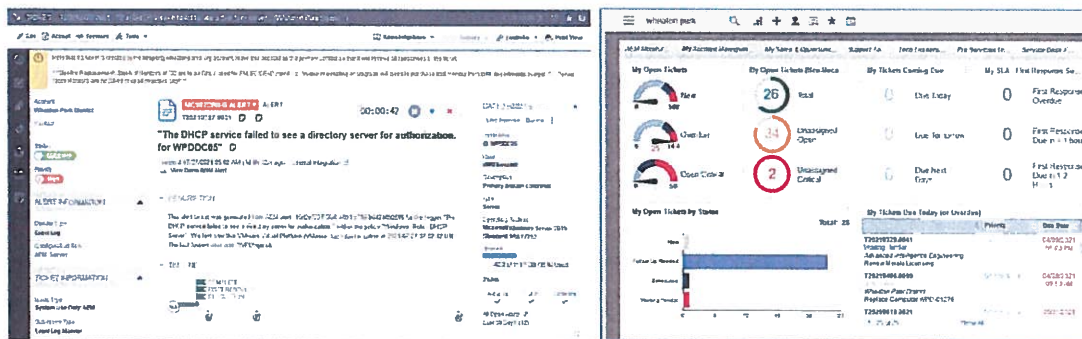
3.1 PROJECT AND SERVICE DELIVERY PLATFORM

Advanced Intelligence Engineering has invested heavily in Autotask, an industry standard ticketing and project management software that allows us to have an automated and streamlined workflow. The AIE team has invested thousands of hours into building out and managing processes within these tools to ensure that client service requirements are met, both in project delivery and at the service desk.

Through Autotask, AIE will provide WPD IT staff with access to a user-friendly client portal. This portal will provide WPD staff with visibility into tickets, projects, and project tasks.

3.1.1 Service Delivery in Autotask

The service desk portion of Autotask allows AIE to track tickets from their initial creation to their completion, ensuring regular follow-up occurs, time is tracked, and the client is consistently kept up-to-date. AIE uses an email parser to create automatic tickets, making ticket correspondence as simple as sending an email to our staff. WPD IT staff can also create tickets via the client portal, and individual users will have an easy-access system tray on their workstations to create a ticket via email in both systems.

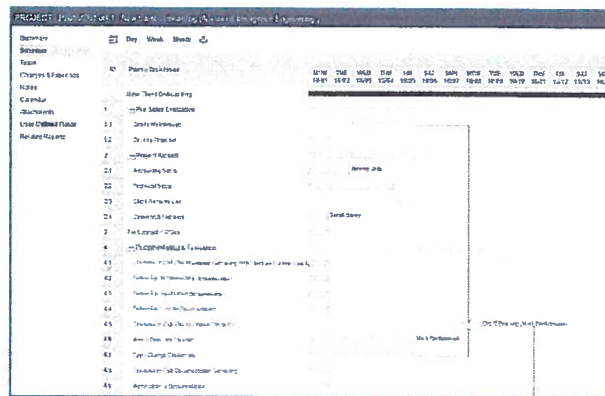


Trouble tickets (see screenshots above) are always assigned to a specific engineer, who is able to easily track work on that specific issue, ensuring that internal desktop issues are only addressed by AIE when requested. The Autotask tool also allows for live data on ticket performance, ensuring that all engineers are able to address tickets quickly and that nothing falls through the cracks.

3.1.2 Project Management in Autotask

Autotask allows AIE to manage projects in a streamlined fashion. From project proposal design stage all the way through to completion, Autotask tracks a project with real time data, including hours worked, tasks completed, open issues, affected successor tasks, and specific schedule and follow-up items.

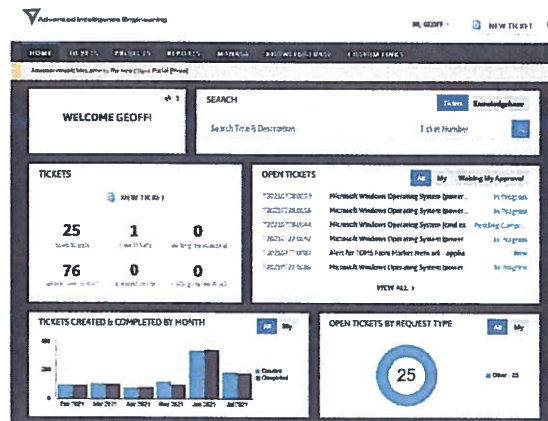
AIE's project manager is able to use the project management tool (pictured above) to provide Gantt charts, regular status updates, and track unexpected issues as they arise.



Additionally, AIE drives projects using Autotask's live metrics on all projects, ensuring project budget and delivery time frames align.

4 CLIENT PORTAL

AIE provides a client portal with fully customizable access levels for clients. Decision makers have access to all ticketing information, project information, invoices, and asset tracking. End-users have access to all tickets currently in progress under their contact. The portal allows for easy communication between AIE and the client.



To increase user-friendliness, AIE provides fully integrated email communication, allowing AIE and the end-user to update the portal via email. A convenient icon is placed in the system tray of each PC on the client network. AIE staff can work with designated WDP contacts to create client-specific “quick ticket” templates, increasing the user-friendliness of the portal.

5 SUPPORT HOURS

5.1 BUSINESS HOURS (7:30AM – 5:30PM, M-F)

AIE staffs the help desk during regular business hours, including phones, email, and client portal support queues. During business hours, AIE follows a priority-based SLA approach, as outlined below. Using live reporting tools, AIE is able to ensure that SLA response times are met or exceeded by technical staff.

TROUBLE THRESHOLD	PRIORITY	FIRST RESPONSE TIME
General Network Down Internet Down Major Server Down	Critical	1 business hour
General Network Impaired Department Down Minor Server Down Major Application Down Major Device Down VIP Down	High	2 business Hours
Localized Network Impaired Department Impaired VIP Impaired Any Person Down	Medium	4 business hours
Any Person Impaired Minor Device Down Minor Application Down Required Re-Configurations	Low	1 business day
Maintenance Upgrades Non-Critical Vendor Calls	When Convenient	2 business days

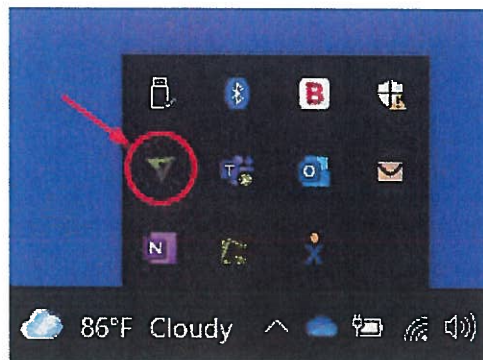
5.2 AFTER HOURS, WEEKENDS, AND HOLIDAYS

Given the fact that many important services rendered by WPD in the community occur during evenings and weekends, AIE understands that WPD will have after-hours support requirements. AIE provides on-call engineering staff on weekends, holidays, and after hours. Management staff ensure that on-call emergencies are dealt with in a timely manner.

On-call engineers can be reached by calling the standard support desk number. After hours support is available for trouble tickets at a critical or high priority threshold; AIE's strategy is to stabilize the situation, reduce the trouble threshold, and provide any additional support during regular business hours.

6 REMOTE SUPPORT TOOLS

AIE uses a suite of tools that integrate tightly with our service desk and project management system, Autotask. Our Remote Monitoring and Management (RMM) product is a sister product of Autotask called Datto RMM. AIE staff remediate any discovered or reported issues remotely wherever possible, which enables streamlined, flexible and rapid support to end users and the technology infrastructure at WPD.



Additionally, WPD IT staff and end-users will have easy access to our support system through both the AIE icon in their PC's system tray and through AIE's client portal.

7 ONSITE SUPPORT

AIE engineering staff will work in conjunction with AIE service desk administration staff and appropriate client contacts to schedule onsite visits when remote support to correct an issue is not an option. Given the size of the WPD network and our location central to WPD's various facilities, we expect to provide regular onsite service, which will enable our engineers to get to know the WPD staff better and identify needs on a more personal level.

8 PROACTIVE MONITORING TOOLS

8.1 NETWORK MONITORING TOOLS

Advanced Intelligence Engineering utilizes industry standard monitoring software for ongoing network and systems monitoring and support. These tools include Datto RMM for workstation and server management, and a combination of Auvik and the Cisco Meraki administration portal for network infrastructure management. Additionally, Datto's BCDR portal is used to remotely administer our backup and disaster recovery appliances, and BitDefender is used to provide malware protection on all server and workstation endpoints. All of these tools integrate with Autotask to automatically create alert tickets within the AIE ticketing system. AIE technical staff monitor all alerts during normal business hours, and alerts of a critical priority will automatically notify the on-call engineer or emergency situations after-hours.

8.1.1.1 Server/PC Health Monitoring

The RMM agents monitor uptime, CPU/Disk/Memory usage, operating system services, and connectivity. Engineers watch for monitoring-generated alerts during business hours to respond within SLA timeframes.

8.1.1.2 Anti-Malware Status Monitoring

Managed anti-virus is included for all servers and workstations using BitDefender. This anti-virus solution maintains definition updates, scan engine updates, and scan scheduling. When a virus is detected and quarantined, AIE staff are notified to take remediation steps to confirm that the threat has been cleared in its entirety.

8.1.1.3 Backup Status Monitoring

The Datto BCDR portal monitors the success of all backups for covered servers and workstations. This sends alerts into Autotask in the event of a backup failure, enabling AIE staff to find and remediate a backup problem before it becomes a disaster recovery issue.

8.1.1.4 Remote Access

The RMM agent also includes integrated remote access through four distinct remote access tools, allowing multiple means of accessing systems in the event one or more remote access methods fail. This allows AIE and WPD staff remote access to devices for support, enabling them to address alerts without interrupting the end-user or coming onsite.

8.1.2 Network Monitoring

AIE monitors network activity through Auvik and the Meraki administrative portal to provide insights into the health and utilization of the entire network. This provides the ability to identify developing problems early and to identify any links in the network that are insufficient for daily business needs, allowing AIE to provide recommendations for upgrade or replacement when needed.

8.1.3 Security Monitoring

The sophistication of today's cyber-security threats is such that traditional antivirus software must run in conjunction with additional tools in order to provide sufficient protection for the network. Every organization is vulnerable to attack at any time, which is why AIE provides additional security services

through RocketCyber. This service continually monitors the desktops, laptops, servers and network devices for evidence of intruders, sending the results to a live team of security engineers who analyze the data and alert AIE if there is evidence of malicious activity. Affected systems can be removed automatically from the network for additional remediation work if necessary, disrupting the activities of potential threat actors before a cyberattack can be launched.

Additionally, AIE utilizes a dark web monitoring service that provides sophisticated, analyst-validated dark web intelligence combined with cutting-edge live search capabilities enabling AIE to identify compromised or stolen credentials in order to close the gap on a breach before it happens.

9 SYSTEM DOCUMENTATION

AIE believes that documentation is about the network equipment and inventory, but also about the health of that equipment. Therefore, AIE maintains documentation on the full client network via quarterly health reports. These health reports and documentation can be provided on demand as well.

9.1 PASSWORD DOCUMENTATION

AIE utilizes ITGlue, a product widely recognized as a leader in IT documentation and password storage. With granular, per-account / per-engineer security, AIE is able to easily track who has accessed specific client passwords, restrict access on a client or password level to certain personnel, and globally change active directory passwords if a security concern requires it.

AIE can provide WPD staff with client-facing, read-only access to the ITGlue password management and documentation portal, for secure and streamlined password sharing.

10 CROSS TRAINING TO MINIMIZE RISK

AIE assigns multiple personnel to any given client account, providing greater opportunity for exposure and cross training in order to ensure that clients see little to no disruption in service at any given time. AIE maintains careful documentation of client networks, processes, and open support issues to allow for this seamless experience. When transitions occur, AIE schedules regular meetings and provides ample time for training and hand-off.

Should any key personnel change, AIE will provide a resume of the new personnel to the WPD staff for approval, as requested.

11 CONSISTENT COMMUNICATION

Clear and reliable communication is one of AIE's core values as an organization. We understand that our clients will only be as happy with their IT support as they are with our communication. Through our ticketing system, we keep our clients up-to-date on each incident as it progress. When needed, our management team will step in to provide extra levels of client communication. Similar processes are followed for project communication. Additionally, AIE will hold monthly vCIO meetings with the WPD leadership to discuss strategic plans.

11.1 DAY-TO-DAY COMMUNICATION

Our engineers keep clients regularly up-to-date with ticket updates in the client portal, as well as through phone and email correspondence. Onsite visits on an as-needed basis also serve an integral role in keeping regular communication with the client.

11.2 MANAGEMENT TEAM

While much of the day-to-day communication comes from AIE's engineering staff, our account management team makes it a priority to build a relationship with each of our clients. Our Service Deliver Manager is actively involved in overseeing incidents, work orders and projects through to completion, spotting red flags quickly and communicating with the client. He welcomes phone calls with questions or concerns. Our account manager communicates actively with key account contacts to ensure that the big picture IT concerns are being addressed.

Account Manager

As principal of AIE, *Jeremy Wills* serves as account manager of key client relations. Throughout Jeremy's work tenure, he has served in various sales, client service, and management roles within the technology space, responsible for the management of budgets, as well as corporate IT direction. Jeremy has directed the development of AIE's client service philosophy, seeking to develop a company culture that puts the clients' needs first, always emphasizing the strong values of compassion, competency, and communication. Jeremy holds a BA in Telecommunications, from Baylor University.

Service Delivery Manager and Project Manager

Geoff Pearson serves as Service Delivery Manager and Project Manager, managing client service and AIE internal processes, workflow and support tool integration. Geoff possesses over 15 years' experience in IT, including desktop, server and network administration, IP telephony support, and IT project, account, and service management. Geoff has served in several capacities at AIE, including that of a systems engineer on the support team, support team lead, and for the past two years as head of the service department in the role of Service Delivery Manager.

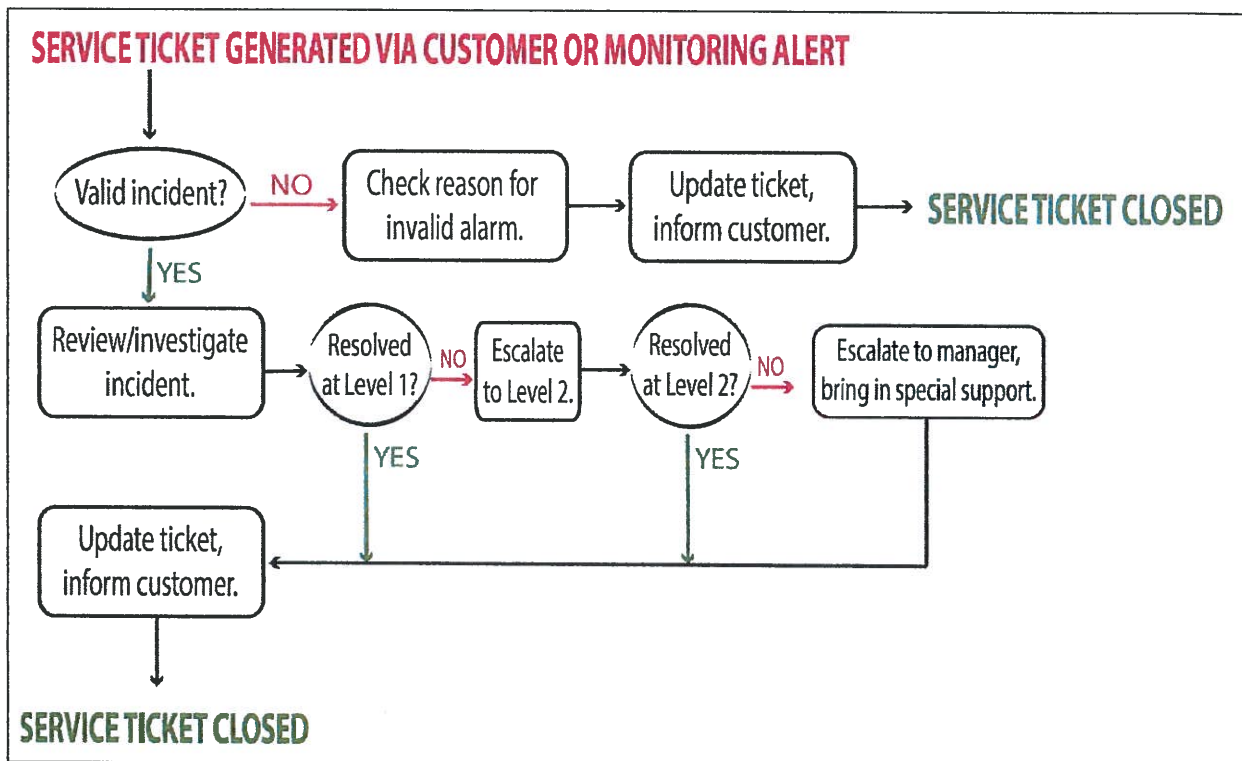
11.3 ACCOUNT REVIEWS

AIE's management team will conduct regular business reviews with key WPD leadership. The reviews will be driven by a list of open items and supplemented with reports of network performance, service deliver, or other items as needed. The reviews will include the opportunity to address such items as budgets, priorities, and upcoming projects. They will also include opportunity to discuss upcoming business needs and the long-term technology strategy to enable growth and efficiency for WPD's operations.

12 TROUBLESHOOTING / VENDOR MANAGEMENT

12.1 OVERVIEW OF SERVICE MANAGEMENT WORKFLOW

The AIE service desk workflow is illustrated at a high level in the following diagram.



12.1.1 Ticket Creation and First Response

Tickets are created in the AIE service desk system in a variety of ways. They can be created automatically by a monitoring alert from our advanced remote monitoring and management (RMM) tools, automatically on a recurring schedule for regular services such as server maintenance, or by customer request via e-mail, phone, or secure client portal. First response SLAs are in place based upon ticket priority.

While most service requests are submitted during standard business hours, AIE maintains an on-call rotation of engineers who are responsible for handling after-hours support calls. All after-hours tickets

requiring emergency support must be requested via phone. Voicemails left at the AIE Help Desk create an automatic ticket, and the call will be returned within one hour by the on-call technician.

12.2 SERVICE LEVEL AGREEMENTS / ESCALATION THRESHOLDS

AIE maintains the following SLAs for escalation thresholds.

TROUBLE THRESHOLD	PRIORITY	ESCALATION THRESHOLD	RESOLUTION TIME
General Network Down Internet Down Major Server Down	Critical	2 business hours	ASAP – Best Effort
General Network Impaired Department Down Minor Server Down Major Application Down Major Device Down VIP Down	High	8 business hours	ASAP – Best Effort
Localized Network Impaired Department Impaired VIP Impaired Any Person Down	Medium	2 business days	ASAP – Best Effort
Any Person Impaired Minor Device Down Minor Application Down Required Re-Configurations	Low	4 business days	ASAP – Best Effort
Maintenance Upgrades Non-Critical Vendor Calls	When Convenient	N/A	Best Effort

“Escalation Threshold” is defined as the time at which an unresolved incident without a defined plan for resolution will be escalated to a higher support tier. This does not apply to those incidents waiting for materials, waiting for response from client or vendor, or with scheduled remote or onsite service calls.

“Resolution Time” is defined as the time within which AIE will resolve the issue. This resolution may, include a suitable work-around until long-term change, which may or may not be covered under this Agreement, can be made. Due to the nature of situations and networks, AIE does not guarantee any specific Resolution Time, but does guarantee Response Time and Escalation Threshold.

13 PROACTIVE SUPPORT

AIE follows a proactive support model to our network management, including hardware and software maintenance levels, automatic updates, and careful application of new security patches. Our philosophy is that preventive network care is far more effective than a merely reactive mentality.

13.1 VENDOR SUPPORT MAINTENANCE

AIE has live data feeds that inform our procurement team when client network devices have expiring warranties, service contracts, SSL certificates, or licensing subscriptions.

Our staff reaches out to our clients when warranties or contracts are expiring, with quotes for renewal when applicable. Our system also lets AIE staff know when they are supporting a device with no warranty, to facilitate informed decision making and cost analysis of the repair versus replacement of the device.

13.2 UPDATES AND NEW FUNCTIONALITY

As updates and new functionality become available, AIE works with the client staff to determine new best practices and any network changes that may be required. AIE's engineers apply patches as appropriate for our client's environment when completing the monthly maintenance. AIE schedules automatic updates for workstations at a time convenient to our clients.

This maintenance is tracked and monitored in our ticketing system, providing an ongoing record of the updates performed on each server, workstation or network device. Should updates fail to apply correctly, AIE's ticketing system records this, and staff address it promptly.

14 STRATEGIC CONSULTING AND BUDGETING

The purpose of reporting, monitoring, and IT support is never to be an end in itself. AIE uses this information to provide clients with CIO-level IT consulting, built on AIE and industry standard field-proven methodologies.

AIE uses network tools, documentation, direct observation, and interviews to review an IT environment for potential risks and/or opportunities for improvement. We identify these risks and opportunities for improvement with a traffic light system that flags observations as green, yellow, and red.

GREEN	From no to mild risk – no immediate issues and/or minimal consequences
YELLOW	From mild to medium risk – will require attention in the next 3 months and/or not aligned with best practices.
RED	From medium to urgent risk – imminent issue and/or serious consequences

Throughout each of the areas reviewed in this assessment, AIE targets three core pillars that we call SMB IT:

- Secure IT – Can it be secured, and how do you know it's secured?
- Manage IT – Can it be managed, and how do you know it's managed?
- Back IT up – Can it be backed up, and how do you know it's backed up?

AIE offers this IT Assessment to provide suggestions on how the IT environment could be enhanced to better support these business goals. In our initial client assessments, we determine where the client falls in each of the three pillars. Then, using the structured model as a guide, we work with the client to set long-term and short-term technology goals, addressing needed services and products, or

improvements to the existing infrastructure. AIE engineers provide a true rationale for any IT investments, using technology to grow the bottom-line, not take away from it.

Here's an example of the traffic light system:

Backups	Image-level local backups for all servers	Passed
	Local backups stored to NAS device	Passed
	Critical <u>on-premise</u> data backed up to cloud	Passed
	Office 365 data is backed up	Needs Attention
Switching/Cabling	Disaster recovery plan in place	No DR plan
	Switching hardware under support contract	2 Near EOL
	Switches support SNMP monitoring	Passed
	Switches are Layer 2 / Layer 3	Passed
	Cabling is Cat5e or above and <u>run in</u> single runs throughout	Needs Attention
Wireless	Cables are terminated and labeled	Needs Attention
	Wireless has a central controller	Passed
	SSID's are secured with proper encryption	Passed
	Corporate SSID is only in use on company devices	Passed
	Adequate wireless coverage exists for business needs	Passed
Firewall/Router	PoE is powered by a switch (not PoE injectors)	Passed
	Firewall hardware under support contract	Passed
	Firewall firmware is <u>up-to-date</u>	Passed
	Firewall supports failover Internet	Passed
	Open external ports have documented business justification	Passed
Internet	Sufficient bandwidth, with minimum 50 Mbps / 10 Mbps	Passed
	Failover Internet is in place (minimum 10 Mbps / 3 Mbps)	None
	Static IPs (just one, or multiple?)	Passed
Workstations	PC replacement plan keeps workstations within one year of warranty exp	Needs Attention
	All workstations are running Windows 10 Pro	Passed
	Workstations have minimum 7.9 GB RAM, i3 processor	Failed
Servers	Workstations are joined to the domain	Passed
	Servers have active warranties in place	Passed
	Servers are running a minimum of Server 2012 R2	Passed
	Virtualization is in place	Passed
	Redundant power in place for all physical servers	Passed

15 EQUIPMENT DISPOSAL

AIE's processes for equipment disposal are focused on protecting the environment and reducing costs for the client, while protecting secure information that may still be stored on old devices.

When old equipment is ready to be retired, AIE engineers first ensure that all necessary data has been removed. Once receiving approval to retire the device, our engineers take necessary precautions to prevent unwanted or malicious data recovery.

AIE partners with electronics recycling companies that can responsibly dispose of equipment and provide certificates of destruction for hard drives and other devices storing sensitive data. We also work alongside clients who have specific compliance needs for disposal ordinances, and our technicians document equipment designated for recycling as it is retired from service.

16 DETAILED RECORD KEEPING

AIE's technicians and engineers are required to keep detailed records of work performed on each ticket and during each task of a project. By default, we track the resource, date worked, summary notes, and hours worked. Additional details tracked include metrics such as the asset, the client ticket contact, the issue, and the billed rates. Reports can be generated on demand and delivered to the client either upon request or on a pre-scheduled basis.

T20140904.0017		Sept. Server Maintenance	
		Progress Made:	
		Installed appropriate Windows Updates	
		Installed 3rd party vendor updates	
		Scheduled a reboot during the maintenance window	
		Verified a successful after-hours reboot	
		Reviewed event logs (created tickets as needed)	
		Ran CCleaner	
09/04/2014	Becker, Mark	Ran Malwarebytes Antimalware	1.00
		Reviewed Managed Antivirus quick and deep scans	
		Reviewed backup logs	
		Tested the backup restore on any month-old files	
		Reviewed available disk space	
		Updated server maintenance notes	
		Next steps: none	
		Ticket Total	1.00
T20140905.0007		Reinstall Filemaker operating system	
		Progress made: Installed Windows 7 Ultimate on a VM on DC01. Began testing of	
		Filemaker image restore to VM to try repairing Filemaker rather than re-installing.	
09/04/2014	Kaiser, Stephen	Next steps: Copy Filemaker database to Filemaker-Test and try accessing	1.50
		database. Get Windows to restore an image to the Filemaker-Restore VM.	
		Ticket Total	1.50

17 ONBOARDING METHODOLOGY

17.1 APPROACH

AIE's onboarding process is streamlined and tracked as a project through our project management system. WPD staff will be granted access via the client portal to view onboarding project progress.

17.1.1 Assessment

AIE will assess the network with industry standard network diagnostic tools and an on-site visit to the primary locations. These assessments will be discussed with the client in a pre-onboarding meeting, designed to identify and determine any potential problem areas or changes that should be made prior to contract start date. AIE will work with the incumbent vendor to transfer custody of relevant materials, such as system passwords and hard disk keys.

The initial site survey will include documenting the following WPD network policies:

- Workstation Installation Checklist and Documentation
- Application Installation Checklist, Automation and Documentation
- User Account Provisioning Documentation and Forms
- Network Security
- Server and Workstation Backup Routines and Performance
- Virus Protection
- Spam Filtering
- Hardware Integrity (check for pending failures)
- System Performance and Trends
- Overall Network Design and Layout

If, during the initial assessment process, AIE finds that WPD's network requires changes to meet minimum compliance standards in order to provide the level of support detailed in this proposal, AIE will identify the changes necessary and provide WPD with a project proposal.

17.1.2 Initiating Service

Following assessment, AIE will begin the service initiation process. This process will include the following steps:

- An AIE engineer will prepare a customized version of the RMM agent to install on each workstation and server. AIE will assign an engineer to be onsite at each client location to install an RMM agent on each workstation and server.
- Working with the client's preferences and the data gathered during the assessment phase, AIE will set up backup software and monitoring scripts and settings.
- AIE will meet with the WPD team to verify the appropriate technical data, gain understanding of environment and current open issues, tickets and problems.
- AIE will schedule initial meetings with designated WPD contacts for consulting phone calls and business reviews.
- AIE will schedule a training session with the WPD IT staff to facilitate the transition to the AIE Help Desk for support calls.

17.1.3 Billing

AIE requires the first month's recurring service fees and the onboarding fee to be paid prior to contract start. Ongoing recurring service fees can optionally be paid on monthly ACH auto pay. AIE invoices additional labor charges on a weekly basis.

17.1.4 Contractual Agreement

AIE will require WPD to sign our standard managed services agreement (sample attached) before initiating work.

17.2 TIMEFRAME

AIE understands that the Wheaton Park District anticipates an onboarding deadline of December 31, 2021. AIE is fully prepared to meet this deadline.

18 PRICING

18.1 FIXED MONTHLY PRICE

Services	Description	Monthly Price	Changes?
Desktop Support (includes onsite support)	175 workstations	\$17,500	<i>Additional \$100 per month per workstation added</i>
Server Support	16 Servers (3 Host, 13 VM)	INCLUDED	N/A
Network Support	10 locations (cameras, printers, switches, access points)	INCLUDED	N/A
Communications Support	Phones, ISP, POTs lines, fax	INCLUDED	N/A
Vendor Support	Third party application support	INCLUDED	N/A
vCIO Services		INCLUDED	N/A
FIXED MONTHLY TOTALS		\$17,500	

18.2 OTHER MONTHLY SERVICES AND CHARGES

Services	Description	Price
Antivirus	Enterprise antivirus software on all workstations and servers	INCLUDED
Mail Archiving	30 year mail archiving	INCLUDED
Dark Web Monitoring	Credential monitoring service	INCLUDED
Managed SOC	Endpoint, network and cloud threat detection monitoring and 24X7 SOC services	INCLUDED
Email Awareness Training	Training videos and simulated phishing emails	INCLUDED
Client Ticket Portal		INCLUDED
Datto Backup	1 SP4000 and 1S4E6 backup and disaster recovery services	\$1,217.90 / MO
Microsoft Licensing	Office 365 Licensing	Charged Separately

18.3 OTHER FEES

Services	Description	Price
Onboarding Fee	See Section 17: Onboarding Methodology	INCLUDED
Onsite Support	Onsite support as needed for troubleshooting	INCLUDED
Travel/Dispatch Charges		NONE
After Hours Support	Non-Business Hours: 5:31p-7:29a M-F, Weekends, 10 Standard Holidays*	\$225/hr
Out of scope support	Normal Business Hours: 8am-6pm M-F	\$180/hr
	Non-Business Hours: 6:01p-7:59a M-F, Weekends, 10 Standard Holidays*	\$180/hr
PC Upgrades	Computer replacements	\$250/PC
Projects	Fixed Fee: Additions to existing network. Upgrades to network hardware, servers and/or server-based applications.	\$190/hr

Exhibit C



Advanced Intelligence Engineering

www.AIE195.com

We have prepared a quote for you

WPD - AIE Managed IT Services Agreement

Quote # JW002257 Version 3

Prepared for:

Wheaton Park District

Prepared by:

Jeremy Wills

Wednesday, December 29, 2021

Wheaton Park District
Mike Benard
1777 S Blanchard St
Wheaton, IL 60189
mbenard@wheatonparks.org

Dear Mike,

Wheaton Park District has extended the opportunity to Advanced Intelligence Engineering via RFP for a partnership between our two organizations. Our proposal aims to demonstrate how we will effectively manage, monitor, shape and position the IT environment as a foundational driver for the success of WPD's organizational vision which is to "commit to service excellence, financial stability and an enriched quality of life for our stakeholders. We accomplish this through continuous improvement of people and systems while living our values."

We strongly believe strongly we can deliver on all areas required to provide a strong partnership that will continue to reinforce the mission of WPD. These areas include the following:

- Monitoring and management of internal systems and the network
- Facilitation of a quality working relationship with WPD's leadership team in order to properly support end-users within the organization
- Delivery of quality CIO services focused on alignment of the Park District's technology investments to their organizational goals
- Capable project management demonstrated through a commitment to a shared vision, strong leadership, proper delegation and consistent communication

In addition, our MSP Agreement details the following areas:

- AIE's Service Level Agreement
- Minimum Standards
- Excluded Services
- The On-boarding Experience
- AIE's Monthly Recurring Services
- Labor Rates
- Fees & Payment
- AIE's Master Services Agreement

Thank you for your consideration.

Regards,



Jeremy Wills
President
Advanced Intelligence Engineering

Network Management

24x7x365 Remote Monitoring & Automated Reporting

AIE uses industry standard tools to monitor network equipment, including firewalls, routers, and switches. Client networks are monitored 24x7x365 AIE also provides detailed network information to a designated client contact.

Network Management

AIE manages the client network equipment. This includes as-needed review of router, switch and firewall logs (where available), and troubleshooting of problems, and performance management. AIE aids our clients in purchasing necessary licensing for network security equipment. AIE also manages the necessary patches for network equipment.

Online Management Tools

AIE makes IT management tools available to all clients as part of managed plans. These tools include an advanced asset management system; a full ticket support system with the ability to track tickets against users, assets, and locations; and online software license management. All of these tools will be configured according to AIE's standard process, with workflows customized to meet each client's unique support needs.

Network Documentation

AIE creates and maintains a network diagram of each client network, along with configuration and network policy information. In conjunction with client staff, AIE maintains a knowledge of client network policies and offers recommendations for best practice improvements. AIE manages all passwords in a securely encrypted location, which in turn can be made available to designated client staff.

Backup Management

AIE offers a complete backup solution with local and cloud based replication and disaster recovery options. Alternatively, clients may use a variety of other backup and disaster recovery solutions, including local NAS, SAN, or tape drive systems, cloud backup, and backup to offsite locations. AIE monitors the success of data backup, performs regular tests of the client's backup system, and manages local backup devices on an ongoing basis. As needed, AIE assists in file restores for individual users.

Vendor Management

AIE provides vendor liaison services for existing IT vendors as a part of this managed plan. This includes working with vendor technical support in the event of a vendor related issue (e.g. IP phones, software, ISP, printers, etc.), facilitating the vendor's onsite or remote access. AIE also assists in quote procurement and price negotiation with existing vendors.

Procurement Assistance

AIE maintains relationships with several major technology distributors. Most of our vendors have Chicago warehouses, often allowing for same or next day procurement of replacement parts. AIE assists client staff in determining what purchases are needed, and sends quotes to the appropriate client contact for easy online approval of orders.

Change Management

AIE provides change management services to all managed IT services clients, as a part of our commitment to Information Technology Infrastructure Library (ITIL) best practices. Network impacting changes are required to be approved by our change advisory board, which exists to ensure that changes have appropriate business justification, an effective action plan, and a plan for remediation should the change not go smoothly. Provisions for emergency changes are available.

Server Management

24x7x365 Remote Monitoring & Automated Reporting

AIE installs our Remote Monitoring & Management (RMM) agents on all Windows servers. All servers are monitored 24x7x365. Monitoring on Windows OS (virtual/guest or physical) servers includes online status, Windows update status, service availability, antivirus status, resource utilization, and backup status. Monitoring on ESXi (physical/host) servers includes power consumption and status, motherboard resource consumption and status, hard drive health and utilization, RAM and CPU health and utilization, and online status.

Regular Maintenance

AIE provides ongoing maintenance for each Windows server. This maintenance includes the remote Windows patch management, system cleanup, and log file maintenance provided for covered servers. AIE also performs as-needed maintenance for ESXi host servers, to update the operating system and patch the image.

Remote Support

AIE provides phone and remote take-control support for server-related issues, including administration of user accounts, printers and file sharing, repair of failed services such as DHCP or DNS, remediation of issues with LOB applications, remediation of malware, and troubleshooting of backup errors.

Image Backup

AIE will include managed image-level backup (local and cloud) on all servers covered under this agreement. AIE will provide support for the backup system, including monitoring backup success and usage and remediating failed backups. Local backup will be stored on a client-owned storage device capable of supporting RAID and compatible with AIE backup solutions.

Workstation Management

24x7x365 Remote Monitoring & Automated Reporting

AIE installs our Remote Monitoring & Management (RMM) agents on each client workstation, including laptops and kiosk workstations. All workstations that connect to the client network must be monitored by AIE and protected with AIE approved antivirus. Workstations are monitored during business hours, and this monitoring includes resource utilization, Windows update success, and antivirus status and scan results.

Regular Maintenance

AIE provides remote Microsoft patch management and system cleanup for managed workstations.

Microsoft Application Support

AIE provides support for client staff using Microsoft applications on a managed workstation, including Microsoft Office 2013-2019 / Office 365. AIE also provides regular patch management for Microsoft applications on all managed workstations.

Other Application Support

AIE provides help desk support for client staff on LOB applications, to ensure these applications are functioning as deployed. AIE can perform patch management on many line of business applications when specifically contracted with the client.

Anti-Virus & Anti-Spyware Management

AIE provides managed antivirus for all managed workstations. AIE manages this antivirus as part of the included monitoring. In the event that a virus is caught and quarantined, AIE uses additional scans to verify all traces have been removed, in compliance with industry standard best practice. AIE also administers an email threat training program for all client end-users, including simulated phishing campaigns and online training tools.

Assistance with End-User Devices

AIE understands that in an increasing BYOD (Bring Your Own Device) world, client employees require ongoing support for their cellular devices, including smart phones. BYOD devices must be connected to a guest network if they are not managed by AIE. AIE provides basic support for guest wireless and email connectivity for client employees.

In order to facilitate a quality support experience, client agrees to keep spare workstations at a ratio of no less than one spare computer per 25 users.

Security Management

Threat Detection Monitoring

AIE employs a managed SOC (Security Operation Center) service that leverages a threat monitoring platform capable of detecting malicious and suspicious activity across three critical attack vectors: endpoint, network and cloud (e.g. O365). This service is comprised of a live team of security experts who proactively monitor activity throughout the entire network for any indication of security threats. AIE and the managed SOC work together to perform the triage of detected activities and work together for remediation when an actionable threat is discovered. This service is designed to mitigate the risk of real time threats including hacking, data exfiltration and ransomware.

Anti-Malware Monitoring

Managed anti-virus is included in AIE's service contract agreements. Scanning schedules, anti-virus engine updates and virus definition updates are all managed from a central source. When a virus is detected and quarantined, AIE staff are notified and can perform additional scans to ensure that no traces of infection remain.

Security Awareness Training

AIE implements and manages periodic, simulated phishing attacks coupled with security awareness training campaigns as part of service contracts. These simulations and training campaigns educate a client's employees on cybersecurity practices and practical steps that can be taken to avoid phishing attacks or other forms of network breaches.

Security Vulnerability Scans & Reporting

AIE analyzes the security posturing of our clients' networks via routine security vulnerability scanning. This ongoing scanning detects external vulnerabilities, anomalous logins, and other abnormal activity, and it provides a convenient means of assessing a network's security policies, any data containing PII, share permissions and more. Scan results are then reviewed and any needed remediation steps identified, which in turn are presented to clients as action items during business reviews.

Spam Filtering

AIE provides spam filtering services in order to detect and quarantine spam, messages with malicious attachments, info-mail, and other threats or nuisance messages, preventing them from filling your users' email inboxes.

Dark Web Monitoring

Hackers and other threat actors harvest credentials from users through phishing attacks, keyloggers, and other means. These credentials are valuable because they represent a potential entry point into a company's network, so many of these credentials are re-sold on a black market that has become known as the Dark Web. AIE helps protect against this vulnerability by implementing Dark Web Monitoring, which watches various known sources of stolen credentials and alerts our staff if a username from your company's domain is detected. This provides a warning so that compromised passwords can be changed, thereby blocking malicious use of the exposed credentials.

Office 365/Cloud Backup

Data stored in Microsoft 365 needs to be backed up just like data stored on a server in your network closet. AIE provides backup services for data stored in Microsoft 365, including e-mail, SharePoint/OneDrive data, and more.

2-Factor Authentication

Passwords by themselves are no longer secure enough. Multi-factor authentication is needed in order to secure e-mail and other accounts, and AIE implements multi-factor authentication for all users of Office 365 e-mail along with other e-mail environments and applications in your organization's environment that support it.

■ Privileged Access Management

Many users have administrative access to their computers through the accounts they use on a day-to-day basis, and this represents a significant security risk because of the potential for malicious software to install itself from infected websites or e-mail messages. However, some users need administrative access frequently because of a need to install or uninstall software from their computers. AIE provides a solution through Privileged Access Management service, which provides controlled administrative access on demand to users to install and run pre-approved software while allowing AIE staff to evaluate and approve other requests for administrative access as necessary.

For effective security, services listed here must be deployed throughout the entirety of the client's environment, be it on servers, workstations, in a cloud environment (such as Microsoft 365), in the network infrastructure (routers, switches, and firewalls), or elsewhere. Devices left unmonitored or unprotected introduce a significant risk to security of the network as a whole, and as such they are not allowed in the network without express client acknowledgement of the risk and liability.

Project Management

Project management and project engineering rates are billed at \$190 per hour. Billing for project management engagements require a down payment with subsequent charges occurring at the close of specified milestones.

■ Project Development

Work with client decision makers to determine and document functional and technical requirements for the project. Identify and evaluate potential solutions that may meet the requirements. Engage vendors to confirm requirements and pricing. Develop initial project plan, including phases/milestones and schedule.

■ Kickoff Call

Work with vendors and key stakeholders to schedule kickoff meetings for new project implementations. Review the project timeline, project milestones, project team members, and any prerequisites or impediments to commencing project work.

■ Project Status Meetings

Coordinate and lead regular project status meetings at a cadence that makes sense for key stakeholders and vendors (generally weekly or biweekly). Track the project schedule and tasks and whether any impediments need to be addressed.

■ Project Communication

Facilitate communication between project team members and vendors, especially as it relates to follow-ups from the project status meetings. Ensure that all project team members receive updates to the project schedule and task assignments in a timely manner.

vCIO Services

■ Monthly Review/Recommendation Meetings

AIE meets with key client decision makers on a monthly basis to review network performance and security status, services implemented, support desk performance, and client's business goals to make recommendations aligned with those goals and to review needed hardware and software infrastructure maintenance and/or replacement.

■ IT Budget Planning

AIE participates in ongoing development of long-term IT budget needs and communicates these to key decision makers at client to facilitate long-term strategy planning for network/technology maintenance, improvement, and security.

■ IT Consulting Services

AIE works alongside key decision makers to recommend technology-based solutions to business problems for the purpose of streamlining client's workflows and increasing efficiency.

Service Level Agreement

AIE commits to the following response time service level agreement as a part of our managed IT services agreement.

For the purposes of determining Service Level Agreements (SLA's), AIE separates tickets into different priority categories. Priority is determined by the business disruption. For example, one person not being able to print has minimal business impact if that person is a part-time intern trying to print expense reports. One person not being able to print has significant business impact if that person is in payroll and can't print paychecks, thus affecting all employees.

For the purposes of determining business impact, "down" means that a person or department is unable to do a major business function. "Impaired" means that a person or department has a work-around available to them, or is unable to do a minor business function (e.g. – can't open Excel files from Outlook, but can save them to desktop and then open).

TROUBLE THRESHOLD	PRIORITY	FIRST RESPONSE	ESCALATION & DISPATCH	RESOLUTION TIME
General Network Down Internet Down Major Server Down	Critical	1 business hour	2 business hours	ASAP – Best Effort
General Network Impaired Department Down Minor Server Down Major Application Down Major Device Down VIP Down	High	2 business Hours	4 business hours	ASAP – Best Effort
Localized Network Impaired Department Impaired VIP Impaired Any Person Down	Medium	4 business hours	1 business day	ASAP – Best Effort
Any Person Impaired Minor Device Down Minor Application Down Required Re-Configurations	Low	1 business day	2 business days	ASAP – Best Effort
Maintenance Upgrades Non-Critical Vendor Calls	When Convenient	2 business days	N/A	Best Effort

AIE works to ensure that issues are resolved as quickly as possible, based upon priority. Back-end issues with Microsoft's cloud services are dependent upon the responsiveness of Microsoft support personnel, and AIE cannot guarantee remediation times. Additionally, remediation times on LOB application issues are dependent upon responsiveness of third-party vendor support personnel, and these applications are supported on a best-effort basis.

Minimum Standards

In order for Client's existing environment to qualify for AIE's Managed Services Provider Agreement, the following requirements must be met:

- All computers with Microsoft Windows or Apple Macintosh Operating Systems must be currently supported by Microsoft or Apple, and have all of the latest service packs and critical updates installed.
- Linux servers are supported on a "best effort" basis, and managed services viability evaluated on a case-by-case basis.
- All server and desktop applications and operating systems must be genuine, licensed, and vendor-supported.
- The environment must have a currently licensed, up-to-date and vendor-supported centrally-managed antivirus solution protecting all servers, desktops, and notebooks/laptops.
- The environment must have a currently licensed, vendor-supported, industry-standard backup solution that can be monitored, and send notifications on job failures and successes. AIE requires evidence of a fully functional backup system prior to assuming responsibility for managing data backup.
- The environment must have a currently licensed, vendor-supported, business-grade firewall between the internal network and the Internet, not something designed for small or home office or home use.
- All wireless data traffic in the environment must be securely encrypted with at least WPA2-PSK.
- Where remote Internet access to the network is required, there must be a public, static IP address assigned to the firewall, and remote communications must be encrypted. Unrestricted remote desktop connections are not permitted unless configured to use a certificate with a Remote Desktop Gateway.
- User logins must be unique. Where exceptions are made for shared devices, the accounts must be identified and locked down and risks minimized.
- Administrative accounts must be used only for that purpose and not for normal day-to-day user activities.
- Physical access to servers and network equipment must be secured and controlled, with access restricted to only those who need it to fulfill their job functions. AIE should be provided with a documented method for gaining physical access to equipment when required.
- Client email must be centrally managed with the vendor's spam and phishing protection enabled.
- Client employees adhere to United States federal and Illinois state regulations regarding computer use. AIE personnel are required to report illegal activity to the appropriate authorities. AIE reserves the right to modify this list at any time, particularly as industry standards change and new threats to security are identified.
- Web servers must use TLS 1.2 or higher encryption. Previous versions of TLS are considered insecure.
- Administrator credentials must be provided for all devices or systems to be managed by AIE including but not limited to firewall, switches, access points, storage devices, and Active Directory domain.

Upon contract execution, AIE will work with Client to develop a remediation timeline and Statement of Work for the identified items where minimum standards are not met. Costs required to assist with bringing Client's environment up to these Minimum Standards are not included in the support Agreement and will be treated as project engagement. While remediation timelines may differ per device or software, all remediation shall be completed and/or project engagements specifically designed to bring systems into compliance shall be approved by client's signature no later than 180 days from the contract start date with the intention of having all remediation fully completed within 270 days from contract start date. Support for any out-of-compliance hardware, software, or any other systems impacted by that hardware or software will be considered an excluded service if compliance is not attained within 180 days of the contract start date.

AIE reserves the right to modify this list at any time, particularly as industry standards change and new threats to security are identified.

Excluded Services

Services rendered under this Agreement do not include:

- Support or monitoring services for any device not meeting Minimum Standards as outlined above.
- The cost to bring Client's environment up to Minimum Standards as outlined above.
- Support for any device not covered under this Agreement, including devices on the network but not covered under this Agreement, or service and repair made necessary by such a device.
- Hardware or software upgrades to servers, network equipment, or endpoint devices, or service and repair made necessary by such an upgrade.
- Labor required to add new devices (virtual or physical) to this agreement (i.e., added workstations, added network equipment, additional servers, network re-architecting, etc.)
- Reconfiguration of the existing network architecture, including adding, changing or removing VLAN's, changing server virtualization design, or any task requiring a network architect.
- Implementation or evaluation of new technology vendors.
- Hardware support for any device outside of vendor warranty.
- The cost of any parts, equipment, shipping or courier charges of any kind.
- The cost of any software, licensing, or software renewal or upgrade fees unless specifically stated by AIE.
- The cost of any third party vendor or manufacturer support or incident fees of any kind.
- Failure due to acts of God, building modifications, power failures or other adverse environmental conditions or factors.
- Service and repair made necessary by the alteration or modification of equipment other than that authorized by AIE, including alterations, software installations or modifications of equipment made by Client's employees or anyone other than AIE.
- Service or repair made necessary by malicious acts on the part of a Client employee.
- Service or repair made necessary by Client failure to follow best practices as recommended by AIE.
- Detection of viruses that are not yet recognized by major antivirus vendors.
- Investigative, remediation or reconfiguration work required as a result of a breach to the network from a cyber attack (e.g. malware, phishing, denial-of-service, man-in-the-middle attack, DNS tunneling, SQL injection, zero-day-exploits, and the like).
- Maintenance or upgrades of application software packages, whether acquired from AIE or any other source unless as specified in this Agreement.
- Support for software applications not related to an employee's job function, or for software applications that are not company-approved.
- Programming (modification of software code) and program (software) maintenance unless as specified in this Agreement.
- Training services of any kind beyond those specified within this agreement.
- Auditing of end-user computing behavior, including application usage or file access.
- Website modifications or webmaster services of any kind.
- Reconfiguration of LOB applications, DBA tasks, or software application development tasks of any kind. (AIE works with the client and application provider to ensure that applications are functioning as currently deployed.)
- Penetration testing, recovery of data and/or financial loss, and security remediation beyond policies and controls that have been adopted in client's organization.
- Any services for which the Client requires AIE to possess specific certification.
- Specialty services outside of services AIE considers to be standard network and help desk support.

Onboarding

AIE's onboarding process is streamlined, and tracked as a project through our project management system. Client staff will optionally be granted access via the client portal to view onboarding project progress.

Documentation

In this phase, AIE will document the new client network, including:

- Discovery of all devices on the network and reviewing this inventory list with the client
- Documenting all IT vendors (e.g. ISP's, phone system providers, LOB applications, email)
- Determining after hours support procedures
- Verify and document passwords for all network backbone devices
- Upload a list of all end users into our ticketing system
- Review remote network access policies
- Collect access keys, entry codes to client site
- Perform visual walkthrough, including pictures of IT closet
- Review Microsoft licensing status and make compliance recommendations
- Produce network diagram

Implementation

In this phase, AIE will implement our support services, including:

- Installation of our monitoring and remote access agent on all endpoint devices
- Train key contacts on service desk procedures and service desk management platform
- Provide end-user training as desired (e.g. email instructions, onsite visit, webinar)
- Provide client portal access as needed
- Review outstanding support issues and create tickets for any outstanding issues
- Confirm IMAC (install/move/add/change) checklists with key account contact

Evaluation

In this phase, AIE will evaluate the new client network, including:

- Compare network with AIE's minimum standards
- Compare network with AIE's best practices
- Propose solutions to any gaps identified
- Review network reports and documentation with client
- Determine IT budget and planning for up to three years in advance

Monthly Recurring Services

Description	Recurring	Qty	Ext. Recurring
This agreement is charged per user, and the below mentioned services are included as applicable for every server, workstation, network equipment (e.g. firewalls, switches, etc), and the Office365 environment:			
<ul style="list-style-type: none"> • Infrastructure Management <ul style="list-style-type: none"> ○ Server Monitoring and Management ○ Workstation Monitoring and Management ○ Network Equipment Monitoring and Management • Security Services & Management <ul style="list-style-type: none"> ○ Backup and Disaster Recovery ○ Security Threat Detection Monitoring ○ Security Vulnerability Scanning ○ Dark Web Monitoring ○ Spam Filtering ○ Email Awareness Training & Anti-Phishing Simulation ○ Multi-Factor Authentication for Email ○ Mail Archiving • End-User Collaboration Services & Support <ul style="list-style-type: none"> ○ Unrestricted Remote End-User Support Desk ○ vCIO Services ○ Project Management* ○ Vendor Management ○ Microsoft Account Management ○ Procurement Services 			
*Project engagements and project management services, as outlined in the Agreement, will be provided as needed. Each engagement will be separately scoped to include all costs associated with the engagement.			
End User Fees	\$100.00	175	\$17,500.00
Recurring Subtotal			\$17,500.00

Labor Rates

Description	Recurring	Price	Qty	Ext. Recurring	Ext. Price
Business Hours (7:30am-5:30pm M-F, excluding posted holidays)					
Remote troubleshooting and support for managed workstations and servers during business hours is included in this agreement, unless the problem originates from an excluded service.					
Project Engement Fixed Hourly Rate Minimum half-hour charge; subsequent time billed in 15 minute increments	\$0.00	\$190.00	1	\$0.00	\$190.00

Labor Rates

Description	Recurring	Price	Qty	Ext. Recurring	Ext. Price
Remote and Onsite Support for Excluded Services (Two Hour Minimum Requirement) Remote support time billed in 15 minute increments. Onsite support time includes a minimum two hour charge with subsequent time billed in 15 minute increments.	\$0.00	\$150.00	1	\$0.00	\$150.00
After Hours (5:31pm-7:29am M-F & all day Saturdays, Sundays, Holidays)					
Project Engement Fixed Hourly Rate Minimum half-hour charge; subsequent time billed in 15 minute increments	\$0.00	\$225.00	1	\$0.00	\$225.00
Remote Support Minimum half-hour charge; subsequent time billed in 15 minute increments	\$0.00	\$225.00	1	\$0.00	\$225.00
Onsite Support (Two Hour Minimum Requirement) Minimum two hour charge; subsequent time billed in 15 minute increments	\$0.00	\$225.00	1	\$0.00	\$225.00
After hours support is only available for tickets meeting the Critical or High priority thresholds. AIE reserves the right to stabilize the situation, reduce the priority, and provide any additional support during regular business hours. AIE observes the following holidays: New Year's Day, Good Friday*, Memorial Day, Independence Day, Labor Day, Thanksgiving (Thursday/Friday), Christmas Eve*, Christmas Day, and New Year's Eve*. <i>*These holidays are observed by a half day, with the AIE office closing at 12:00pm, Central Time.</i>					

Fees & Payment

In order to initiate the work, AIE requires a signed copy of the agreement along with 100% down payment on the setup fee and first month of services.

Setup Fee

Fees will include a one-time account setup fee, as specified in this agreement. Setup fee is due before commencement of work. Account setup includes agent loads on network devices, removal of any previous managed service agent devices (e.g. monitoring, antivirus, etc.), setup of backup software, client portal configuration, asset and user report configurations, diagrams, and asset inventory count. This setup fee does not include the configuration of specific files to be backed up. Any additional setup requirements or onsite troubleshooting requested during the setup visit will be billed according to the hourly support rates set forth in this agreement. Account setup fee only covers those account configurations requested and performed during the account setup. Client will be notified by AIE when account setup has been complete.

Monthly Fees

Monthly fees will be billed as outlined in this agreement, invoiced to Client on a monthly basis, and will become due and payable on the first of this month. Any additional Client equipment and/or Client personnel added during the course of this Agreement could affect the monthly fees.

Labor Fees

Hourly rates shall be billed as set forth in this agreement. AIE reserves the right to change prevailing rates at any time, with 30 days written notice to Client. Labor is invoiced on a weekly basis, and is due per Net 20 invoicing terms. Client shall be billed for all requested support, including, but not limited to, responses to alerts and trouble tickets, end-user support, and changes to account setup or service configuration after the completion of account setup. Any and all services requested by Client that fall outside of the terms of this agreement will be considered projects, and will be quoted and billed as separate, individual services.

Client acknowledges and agrees that for any given Contract-Year, at a minimum, Client will be responsible for at least 75% of the monthly service fees described in this Agreement and the Schedule attached hereto, regardless of any changes to the Scope of Services that may occur.

All invoiced fees or portion thereof, left unpaid for more than 30 days may be assessed an additional 2% service charge. Advanced Intelligence Engineering reserves the right to suspend any Services provided under this Agreement if any payment due hereunder is not received within 45 days of the applicable due date.

All payments due hereunder will be paid in US dollars and may be made by company check, bank draft, money order or wire transfer, allowing sufficient time for funds to clear before commencement of the Services.

A \$50.00 service charge will be paid to Advanced Intelligence Engineering by Client for any returned (bounced) checks. To the extent Advanced Intelligence Engineering must engage in collections activities related to any payment due by Client hereunder, Client agrees to be responsible for and pay all costs of such collection, including but not limited to reasonable attorney fees, suit monies and costs.

WPD - AIE Managed IT Services Agreement



Prepared by:

**Advanced Intelligence
Engineering**

Jeremy Wills
(630) 936-4045 x102
Fax (815) 346-5342
jwills@aie195.com

Prepared for:

Wheaton Park District

1777 S Blanchard St
Wheaton, IL 60189
Mike Benard
(630) 510-4945
mbenard@wheatonparks.org

Quote Information:

Quote #: JW002257

Version: 3
Delivery Date: 12/29/2021
Expiration Date: 01/07/2022

Recurring Expenses Summary

Description	Amount
Monthly Recurring Services	\$17,500.00
Recurring Total:	\$17,500.00

Payment Options

Description	Payments	Interval	Amount
Terms			
48 Months	48	Monthly	\$17,500.00

Summary of Selected Payment Options

Description	Amount
Terms: 48 Months	
Selected Recurring Payment	\$17,500.00
Total of Recurring Payments	\$840,000.00
Total of Payments	\$0.00

This Agreement shall commence on the Effective Date indicated above and shall remain in force for 48 months. The Effective Date of the first term (and all subsequent terms) shall be considered the first day of the first month where ongoing IT services are received. Onboarding may occur prior to the Effective Date.

The Term of this Agreement will automatically renew for a subsequent one (1) year term at the end of the natural term, unless either party gives the other ninety (90) days prior written notice of its intent not to renew this Agreement. Furthermore, this Agreement will automatically renew for a subsequent one (1) year term beginning on the day immediately following the end of each subsequent Renewal Term, unless CLIENT gives Advanced Intelligence Engineering ninety (90) days prior written notice of its intent not to renew this Agreement.

This Managed Services Agreement will be reviewed annually, unless otherwise agreed to in writing beforehand. The results of each annual review will determine if any amendments to this Agreement, the applicable Scope of Services, and/or related fees must be made to support the Client's changing environment, or to better serve the Client's current needs. Any changes that alter the scope and fees of this Agreement must be made in writing and attached as an amendment.

This Managed Services Provider Agreement is a Sub-Agreement of the Master Services Agreement (MSA), attached here.

Advanced Intelligence Engineering

Wheaton Park District

Signature: 

Name: Jeremy Wills

Title: President

Date: _____

Signature: _____

Name: Mike Benard

Title: Executive Director

Date: _____