BILL NO. S-26-11-47

ORDINANCE NO. X-_____

AN ORDINANCE approving the purchase of thirty-six months of Computer Services benefitting the infrastructure utilized by the city of Fort Wayne and Allen County for a total cost of $31,274,348 from and through Resultant by the City of Fort Wayne, Indiana,

Whereas, the City of Fort Wayne, City Utilities and Allen County jointly operate computer systems and networks that benefit all City and County Departments.

Whereas, the City and County have utilized a joint service provider for shared computing infrastructure since 1988.

Whereas, the City of Fort Wayne, City Utilities and Allen County wish to jointly contract and share the cost of IT services through Resultant to manage and secure networks, applications, systems and hardware currently running in our environment.

Whereas, cyber threats against local governments, including ransomware, data theft and account compromise, continue to grow in frequency and sophistication, and a successful attack could interrupt public safety and utility operations and expose information entrusted to the City by its residents.

Whereas, the services provided through Resultant extend well beyond help desk support and include network and server infrastructure, data center operations, backup and disaster recovery, cybersecurity, computer and mobile device support, business and geographic information system (GIS) application support, asset management, project management and technology planning.

Whereas, many of these services operate 24 hours a day, 365 days a year, and depend on technology that is continuously available, supported and protected.

Whereas, Amendment Two strengthens accountability by establishing measurable cybersecurity and service performance standards aligned with national guidance from the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), regular performance and security reporting to City leadership, independent penetration testing, the City's right to audit reported performance, and service credits when standards are not met.

NOW, THEREFORE, BE IT ORDAINED BY THE COMMON COUNCIL OF THE CITY OF FORT WAYNE, INDIANA:

SECTION 1. That the purchase of IT Services for the City's computing infrastructure from Resultant for a total cost to the City of $18,576,688 over thirty-six months is hereby approved in all respects. That said purchase will be used to ensure the proper operation and security of the computing infrastructure throughout the City and County. Each entity will be invoiced for the following total amounts over the duration of the contract:

	2027	2028	2029	(3) Year Total
Allen County	$4,259,482.00	$4,239,687.20	$4,198,490.00	$12,697,659.20
Civil City	$4,184,482.00	$4,102,187.20	$4,020,290.00	$12,306,959.20
City Utilities	$2,109,741.00	$2,089,843.60	$2,070,145.00	$6,269,729.60
City of Fort Wayne Total	$6,294,223.00	$6,192,030.80	$6,090,435.00	$18,576,688.80
Contract Total	**$10,553,705.00**	**$10,431,718.00**	**$10,288,925.00**	**$31,274,348.00**

SECTION 2. That the City is authorized and directed to take all action necessary for the purchase and installation through Resultant.

SECTION 3. That this Ordinance shall be in full force and effect from and after its passage and any and all necessary approval by the Mayor.

_____
Council Member

APPROVED AS TO FORM AND LEGALITY

_____
Malak Heiny, City Attorney

This AMENDMENT is incorporated into and made a part of the Master Services Agreement (MSA) by and between the City of Fort Wayne & Allen County, Indiana (hereafter the City/County or The C/C) and Resultant (Service Provider). In the event of any conflict between this Amendment and the MSA (including Amendment 1 and any Exhibit), this Amendment (TWO) shall control with respect to the subject matter addressed herein.

TABLE OF CONTENTS

1 TERMS & CONDITIONS 2
1.1 Terms and Appropriations 2
1.2 Notifcation of Expiration and/or Termination 2
1.3 Key PerSonnel 2
1.4 Definitions & Terms 3
2 SLA AGREEMENT (UPDATES) (2026) 7
2.1 REVISED SLAs/XLAs TABLE 7
3 REVISED POLICY & PROCEDURE / NEW INTIATIVES 18
3.1 Critical Contacts & Numbers List 18
3.2 Annual Awareness Training 18
3.3 NIST and CISA guidlines 19
3.4 Assets: Hardware, Software and InfrastruCture DEFINITION 20
3.5 Disaster Recovery Management & Testing 21
3.6 New Intiatives: Keeping Current with Policy and Procedure 21
4 PROFESSIONAL FEES 22
5 SIGNATURES 23

1 TERMS & CONDITIONS

1.1 TERMS AND APPROPRIATIONS

The Term of this Agreement shall commence at 12:01 a.m., Eastern Standard Time (EST) on JANUARY 1ST, 2027, contingent upon this fully executed (fully signed) Amendment (two) and shall end on DECEMBER 31st, (2029) subject to appropriation by the City/County of funds for this Agreement for such period and unless terminated in writing earlier in accordance with the Master Services Agreement.

1.2 NOTIFCATION OF EXPIRATION AND/OR TERMINATION

Except as provided below, all contract language with respect to contract expiration, termination, notification and/or communication(s) of the same still applies as written and per the active City/County MSA.

Early Termination Fees. For the Term of this Amendment, the early termination fee schedule set forth in Section 6.7.2 of the MSA is replaced with the following. In the event of any termination of this Agreement in whole by the City/County for convenience pursuant to Section 6.7.2 of the MSA, including any termination deemed a termination for convenience under Sections 6.7.3 or 6.7.4 of the MSA, Service Provider shall recover, in addition to all amounts accrued and owing through the effective date of termination, the early termination fee corresponding to the calendar year in which the termination becomes effective:

	2027	2028	2029
Early Termination Fee	$350,000	$350,000	$300,000

All other provisions of Section 6.7.2 of the MSA, including the notice requirements and the fees applicable to termination by service tower, remain in effect.

1.3 KEY PERSONNEL

This section details the key Service Provider personnel the City/County requires to have oversight involvement in the ongoing selection of personnel for the following roles/titles. Please see MSA section 6.24, section 7.2 and Exhibit G for further detail. Roles/tiles listed in this amendment supersede and variance or conflict with roles/titles listed in the original MSA. All other MSA language with respect to Key Personnel still applies.

1. Program Manager
2. Infrastructure Lead
3. Applications Lead
4. Cyber Security Engineer
5. BRM/PM Manager/Lead:

1.4 DEFINITIONS & TERMS

1. **Security incident**: Any event that actually or potentially threatens the confidentiality, integrity, or availability of City/County systems or data, including malware, ransomware, unauthorized access, account compromise, business email compromise, and data exposure.
2. **Clock**: Security monitoring, triage, containment, and notification run 24x7x365, not business hours.
3. **Measurement source**: All measures shall come from consoles the City/County can access (EDR, vulnerability scanner, identity platform) unless otherwise noted.
4. **Exceptions**: Handled through the same documented, City/County-approved, time-limited exception process as patching.
5. **SLA Credit Point Assignments**:
    a. **Point Allocation.** No single SLA/XLA shall be assigned more than twenty (20) of the 100 credit points described in Section 20.6 of Exhibit D of the MSA. Any reallocation of credit points shall be made by written notice at least thirty (30) days before the start of the calendar quarter in which it takes effect and shall apply prospectively only.
    b. **Point Reallocation.** Will be at the City/County's discretion but a review and true up will be conducted annually in conjunction with Service Provider.
    c. **Critical service levels** such as EDR coverage (#1), Known Exploited and Critical vulnerability remediation (#5), and incident notification (#10) may carry service credits per City/County assignment of credit points as outlined in section 20.6 of the MSA and this Amendment.
6. **Frameworks**: These measures align with the latest CIS Controls and NIST CSF as effective as the date of this Amendment.
7. **NOTE**: The City/County is required under Indiana law (IC 4-13.1-2-9) to report cybersecurity incidents to the Indiana Office of Technology within 48 hours. The 1-hour vendor notification in SLA #10 is stated as such so the City/County can meet that obligation.
8. **Service credits**: A reduction in the monthly invoice when a SLA/XLA assigned credit points is missed.
9. **At-risk amount**: The maximum share of the monthly fee subject to credits as outlined in section 20.6 of the MSA. Service Credits are the City/County's sole and exclusive monetary remedy for SLA/XLA failures, without limiting the City/County's termination rights under Section 6.7.1 of the MSA as modified by this Amendment.
10. **Single Root Cause; No Multiple Credits.** Notwithstanding anything to the contrary in this

Amendment or the MSA, where a single incident, event, or failure, or a series of related incidents arising from the same root cause (a "Single Event"), directly or indirectly causes Service Provider to miss more than one SLA/XLA, the City/County shall be entitled to only one (1) Service Credit for that Single Event, equal to the highest Service Credit applicable to any one of the affected SLAs/XLAs. A Single Event that continues across more than one Measurement Period shall be treated as one SLA/XLA failure for purposes of Service Credits, earn-back, and any chronic-failure or termination provision. The determination of root cause shall be documented in the applicable RCA and, if disputed, resolved through the IT Governance process described in Exhibit D, Section 20.5.

11. **Excluded Events**. No SLA/XLA shall be deemed missed, and no Service Credits shall apply, to the extent the failure results directly or indirectly from any of the following (each an "Excluded Event"):
    a. acts or omissions of third parties not under contract to Service Provider, including telecommunications carriers, internet service providers, utilities, software and hardware manufacturers, cloud and SaaS providers, and other City/County vendors;
    b. systems, equipment, software, circuits, or facilities owned, contracted, or managed by the City/County or its other vendors that are not supported by Service Provider under this Agreement;
    c. acts or omissions of the City/County, including delays in providing approvals, access, information, personnel, or resources required under this Agreement;
    d. the City/County's decision not to approve, fund, or implement a Service Provider recommendation, including declined or deferred patches, changes, or upgrades, unfunded replacement of end-of-life or unsupported assets, and approved risk exceptions;
    e. actions taken at the City/County's direction;
    f. scheduled maintenance performed within City/County-approved maintenance windows;
    g. unavailability of vendor patches, fixes, parts, or products; or
    h. Force Majeure events, provided that a cybersecurity incident, including malware, ransomware, unauthorized access, or account compromise, shall not constitute a Force Majeure event or an Excluded Event, regardless of whether it is attributed to a nation-state, state-sponsored actor, terrorist organization, or act of war. Service Provider's obligations for security monitoring, incident notification, triage, containment, and response shall not be suspended during any cybersecurity incident. Physical acts of war or terrorism affecting facilities or infrastructure outside Service Provider's control may continue to qualify as Force Majeure.

For time-based SLAs/XLAs, the measurement clock shall be suspended for the duration of any Excluded Event. In each case Service Provider shall promptly notify the City/County, manage resolution with any responsible third party, and use commercially reasonable efforts to mitigate the impact and restore service. This Section supplements

and does not limit Section 20.6.1 of Exhibit D of the MSA.

12. **Earn-back**: The Service Provider recovers a credit by meeting the missed SLA for a set period as outlined in section 20.6.2 of the MSA.
13. **Critical vs. report-only**: Which SLAs carry credits and which are only tracked, with the ability to move items between the two lists upon mutual agreement.
14. **Chronic Failure**: A "Chronic Failure" occurs when Service Provider fails to meet the same Eligible Service Level in (a) three (3) consecutive Measurement Periods, or (b) four (4) Measurement Periods within any rolling six (6) Measurement Period window. An "Eligible Service Level" is any SLA/XLA assigned five (5) or more credit points. Eligibility shall be determined by the credit points assigned at the beginning of the first Measurement Period counted toward the Chronic Failure; changes in point allocation made after that date shall not apply to that determination. For purposes of determining a Chronic Failure: (i) failures resulting from Excluded Events shall not be counted; (ii) a Single Event spanning more than one Measurement Period shall be counted as one failure; and (iii) failures occurring during any baseline or report-only period shall not be counted.

    Upon a Chronic Failure, the City/County may provide written notice to Service Provider. Within fifteen (15) business days of such notice, Service Provider shall deliver a root cause analysis and a corrective action plan for review and approval by the City/County, which approval shall not be unreasonably withheld. If Service Provider fails to deliver the corrective action plan, or fails to restore performance (with sustained restoration of at least sixty (60) days) of the affected Eligible Service Level within ninety (90) days of the plan's approval, such failure shall constitute a Service Provider Default under Section 6.7.1(d) of the MSA. In that event the City/County may terminate the affected service tower in accordance with Section 6.7.1, and such termination shall be the City/County's sole remedy for a Chronic Failure in addition to Service Credits.

15. **Right to audit**: Service Provider shall provide the City/County read-only access to the reporting data used to calculate SLA/XLA performance. Upon thirty (30) days' written notice, consistent with Section 6.5 of the MSA, the City/County may audit SLA/XLA calculations itself or through an independent third party reasonably acceptable to Service Provider and bound by confidentiality obligations. The City/County shall bear the cost of any audit unless the audit shows Service Provider's reported performance overstated actual performance by more than three percent (3%) for the audited period, in which case Service Provider shall reimburse the reasonable cost of the audit. Any resulting Service Credit adjustments shall be limited to the twelve (12) months preceding the audit notice.
16. **Baseline Period:** Any SLA/XLA that is new or modified by this Amendment shall be measured and reported, but shall not be subject to Service Credits or counted toward a Chronic Failure, for the first sixty (60) days following the Effective Date of this Amendment.

17. **Asset Management:** Service Provider shall have the responsibility and management of the following, as per the agreed upon MSA, Exhibit E, Consolidated Roles and Responsibilities Tables, Section 21.28 "Asset Management and Tracking".

18. **Scope Changes**

    a. **Cybersecurity**: Service Provider will be responsible for running a Cybersecurity Tower compromising:

        i. Facilitating Cybersecurity governance program including security policy development;

        ii. Providing 24x7 security monitoring across the state provided and/or City/County provided SOC tools (e.g. Crowdstrike, Varonis, Mandiant);

        iii. Executing the vulnerability management program;

        iv. Executing the cybersecurity user awareness program;

        v. Executing a dark web monitoring program; and

        vi. Executing an annual disaster recovery test and incident response tabletop exercise.

    b. **24x7 Advanced Support**: Replacing NetFor help desk with Resultant staffed technical support specialists beginning July 1, 2027.

    c. **Mobile Devices**: Service Provider will be responsible for operating the MDM platform for ~1,000 mobile devices across the City/County.

    d. **Formatta:** Resultant will support Formatta throughout the City's migration of forms to CivicPlus. The cost shown reflects an estimated completion date of June 30th, 2028. Fees will be billed monthly at the same rate throughout the migration.

    e. **SLA Changes:** Changes as required by the revised SLA's in section 2 of this Amendment (Amendment 2 / Dec 2026)

2 SLA AGREEMENT (UPDATES) **(2026)**

2.1 REVISED SLAS/XLAS TABLE

The following amended SLAs/XLAs serve to take precedence/replace and supersede the original SLA/XLA table contained in the City/County MSA by and between the City/County and Service Provider.

REMINDER: ALL current MSA Roles and Responsibilities (R&R) tables and Reporting Requirements for each service tower/area and contract management overall not specifically detailed and described as part of this amendment are still fully in effect and required and part of the original MSA terms.

	MSA: SERVICE DESK	Service Measure / Performance Target					SLAs/XLAs
	Measure	**Description**					**SLA**
1	1st Call Resolution Rate	Resolution on first call of **resolvable incidents** *(Excluding calls to the Service Desk not related to technical issues)* Definition: Resolvable means call was resolved to user satisfaction and no follow up is required.					94%
2	Email Response rate (beyond automated responses)	≤ 30 mins (includes time for user to be called or routed to the correct service group/team) NOTE: Review and update annually as new initiatives are implemented					90%
3	Call Routing	1. Service desk appropriately triages service request and routes ticket to the correct service team. 2. NOTE: With respect to user generated tickets only. Not automated ticket triage.					95%
4	Knowledge Base Articles	1. Knowledge Base Articles are to be **reviewed annually correcting for changes when/where needed.** 2. Additionally, **new KBAs should be continually sought** for inclusion in library. 3. Goal: Keep current and keep growing the library.					Report (100%)
	Sev Level SLAs	**Respond Within (business)**	**SLA**	**Plan Within (business)**	**SLA**	**Resolve Within (business)**	**SLA**
5	**Severity 1—Urgent**	30 min	95%	2 hours	95%	24 hours *	**95%**
6	**Severity 2—Critical**	1 hour	95%	3 hours	95%	6 hours	**95%**
7	**Severity 3—Normal**	2 hours	90%	6 hours	90%	8 hours	**90%**
8	**Severity 4—Cosmetic**	4 hours	90%	8 hours	90%	24 hours	**90%**
	(*) Sev 1 Urgent Note: In the event of a significant system failure, an agreed upon resolution timeline can be discussed, per City/County IT leadership consent.						
9	Root Cause Analysis (RCA)	1. Provide RCA report for all Sev 1 within 3 business days of completion of Sev 1 incident.					Report (100%)

	MSA: SERVICE DESK	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
		2. Provide RCA report for all Sev 2 and all Reoccurring Problem Tickets – UPON REQUEST. 3. Report ALL completed RCAs and reconciliation report monthly to City/County IT Leadership. (Part of standard Policy & Procedure activities)	
10	Reoccurring Problem	Reoccuring Problem: Is defined as the SAME user-initiated issue/ticket reopened for SAME problem within a 7-day period. Original ticket # must be listed (referenced) in the reopened ticket.	<5%
11	New User Account	Minimum Sev Level 3 SLA applies	N/A
12	Privilege Changes	Minimum Sev Level 3 SLA applies upon approval by City/County IT Leadership	N/A
13	Emergency Disable Account	Within 30 minutes of authorized request during business hours. NOTE 1: Request may only be made from City/County Director level or higher and/or equivalent. NOTE 2: An HRIS and AD integration project should be considered, planned and implemented to make this SLA much easier to facilitate, maintain and manage.	98%
14	Disable User Account (non-emergency)	Minimum Sev Level 3 SLA applies	N/A
15	Account Review	User accounts are to be reconciled with agency employee records quarterly. Report status quarterly. NOTE: see also section 3.2 "New Initiatives" below for further detail.	Quarterly Report
16	Administrator accounts	Report all new, activated and disabled administrator accounts weekly. (i.e. Active Directory Accounts)	Weekly Report
17	Triggered Satisfaction Survey Response	Service Provider responds to any/all **dissatisfied** survey response by contacting the customer within 8 business hours and conducts service request assessment for continuous improvement purposes. Assessment feedback and improvement data is reported monthly to the City/County.	Report (100%)
18	Annual Customer Satisfaction Survey	Mandatory annual survey process. Users % surveyed should be very satisfied or satisfied. (conducted by **independent** 3rd party Surveyor). Survey content and audience to be mutually agreed upon by the City/County and Service provider. Annual 3rd party survey paid for via 50/50 split of City/County & Service Provider. NOTE: Final % of customer base TBD but minimally 15% required submission rate and/or limit participation to department leads, deputy directors and the like.	Report (100%)

	MSA: SERVICE DESK	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
19	Speed-to-Answer	≤ 60 sec	95%
		After hours' support: • Standard: 7am – 5pm ET • 24-hour support (See list below) 24-hour support includes the following areas: 911, FWPD, FWFD, Radio Shop, Jail, Sheriff, Street Dispatch, Traffic Night Shift, FLP, WPCP and CU Dispatch, Building Mgrs. NOTE: SLA forgiveness is reasonable during Q1&Q2 2027 as Service Provider transitions helpdesk.	
20	Speed-to-Answer (2): Critical Contacts	<5 mins for critical contacts list. Is a defined list – 911, Radio shop, etc.) regardless of day/time this list of names & numbers jumps to top of call queue. (See "Critical Contacts" list below in Section 3.1 NOTE: SLA forgiveness is reasonable during Q1&Q2 2027 as Service Provider transitions helpdesk.	2027: 90% 2028: 95%
21	Request Call Back	Time to call a user back that chose to not stay on hold (< 15 minutes)	90%
22	SLA and ALL contractual Reporting Requirements	Measure and report ALL contractual report requirements (SLA and others) as stated within the timeframes detailed. (weekly, monthly, etc.) (Part of standard Policy & Procedure activities)	Report (100%)
23	XLA: First Level Resolution	% tickets resolved by Help Desk regardless of channel / total incidents and requests resolved without escalation. NOTE: 2027 AI & helpdesk responsibility shift to create new baseline. Then reassess and fine tune in 2028.	Report (100%)
24	XLA: Quarterly Net Promoter Score	Index ranging from -100 to 100 that gauges the customer's overall satisfaction with a service and the customer's satisfaction too the organization delivering the service / (Number of Promoters minus Number of Detractors) divided by (Number of Respondents) times 100	85%

	MSA: DESKTOP	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
1	Urgent Request, new device setup, reimaging single installation or move (1 device)	HIGH PRIORITY - Sev Level 2 SLA applies. Request must be approved by City/County IT leadership (i.e. The Chiefs)	See Sev Levels Table
2	Single device setup, reimaging or move (1 device)	Minimum Sev Level 3 SLA applies	
3	Multi device setup, reimaging or move (2+ devices)	Minimum Sev Level 4 SLA applies	

	MSA: DESKTOP	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
4	XLA: % of all end user devices that are capable of being monitored by vendor.	End user devices monitored in vendor's device management as a percentage of all end user devices in vendor's configuration management database	Yr1: 85% Yr2: 90%
5	XLA: % of failed updates, patches or changes.	Service Provider shall deploy security patches to all in-scope systems within the timeframes defined by severity tier, measured from the date the patch is publicly released. Patches shall be submitted for City/County approval within three (3) business days of release for Emergency and Critical tiers and five (5) business days for all others; time awaiting City/County approval shall not count against Service Provider provided the submission was timely. Compliance shall be measured monthly using the City/County-accessible vulnerability scanning platform (Rapid7, Defender) as the percentage of in-scope devices remediated within the applicable timeframe. Any in-scope device that has not reported to the vulnerability scanning platform in more than fourteen (14) calendar days shall be counted as non-compliant. A device may be excluded from the compliance calculation only if (a) it has been formally retired and removed from inventory, or (b) it is covered by a risk exception that is documented by Service Provider, approved in writing by the City/County, and not expired. An excluded device returns to the compliance calculation when its exception expires.	Report as Defined in Description
6	XLA: % of issues reported vs. self-healing scripts deployed.	% of issues reported that are capable of self-healing vs. self-healing issues resolved by vendor's monitoring and management toolset. Ex: Disk defragmentation, disk cleanup, anti-virus missing, computer restart, service restart, blacklisted process, windows patches missing.	>25%

	MSA: NETWORK & SERVER	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
1	LOCAL Production Applications and Databases uptime/availability	Sun-Sat, 000-2400	99.9%
2	Shared Storage systems	Sun-Sat, 000-2400	99.9%
3	QA/Test Systems & Servers	Sun-Sat, 000-2400	95%
4	Internet Access Availability, to devices within City/County control	Sun-Sat, 000-2400	99.9%

	MSA: NETWORK & SERVER	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
5	LAN availability to devices within City/County control	Sun-Sat, 000-2400	99.9%
6	Wireless Network Availability to devices within City/County control	Sun-Sat, 000-2400	97%
7	Server & network performance management	Continuously monitor server and network capacity and performance and storage capacity for defined threshold alerts and anomalies. (Part of standard Policy & Procedure activities)	Report (100%)
8	Trend Analysis and reporting across all platforms. Capacity change requests - Server & Storage	Monthly analysis reports and interim reports on rapidly developing events and trend identification for all devices capable of being monitored.	Monthly Report
9	Deploy security patches necessary to protect or repair environment vulnerabilities.	See/Adhere to KEV table below in Security Services section / SLA #5.	See KEV Table limits below
10	Deployment: New Server	Virtual server – Within 1 business day of approved change/request. **Sev level 3 applies** NOTE 1: City/County and Service Provider to discuss new initiative to automate gold image builds/deployment of servers. NOTE 2: Exceptions can be approved by the City/County on a case-by-case basis.	See Sev Levels
11	Critical Restore Requests:	1-Hour to begin the restore process. When feasible, follow Disaster Recovery policy and procedure for completion. **Sev 1 SLA applies when feasible.** NOTE: Plans are to be created and approved by C/C for applications with large datasets whose transfer speed approaches or exceeds 8 hours. NOTE: Exceptions can be approved by the City/County on a case-by-case basis.	See Sev Levels
12	Non-Critical Restore Requests	1 day to begin from time of notification by Service Recipient. 2 days to complete. **Minimum Sev 3 SLA applies**	See Sev Levels
13	Backup Services: Server Backup	Tier I – IV: Must follow agreed upon backup policy	99%

	MSA: SECURITY SERVICES	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	SLA
	Endpoint Detection & Response (EDR)		

<table>
<tr><th></th><th>MSA: SECURITY SERVICES</th><th>Service Measure / Performance Target</th><th>SLAs/XLAs</th></tr>
<tr><td></td><td>Measure</td><td>Description</td><td>SLA</td></tr>
<tr><td>1</td><td>EDR Coverage</td><td>Percentage of in-scope endpoints and servers with the approved EDR agent installed and active.</td><td>98% Endpoints on 100% of Servers</td></tr>
<tr><td>2</td><td>EDR on New Devices</td><td>EDR agent installed and reporting before any new or reimaged device is issued to a user or placed into production. (Part of standard Policy & Procedure activities)</td><td>Report (100%)</td></tr>
<tr><td>3</td><td>Agent Health</td><td>Unhealthy, disabled, or tampered agents identified and restored within 1 business day of detection.</td><td>95%</td></tr>
<tr><td></td><td>Vulnerability Management</td><td></td><td></td></tr>
<tr><td>4</td><td>Scan Coverage</td><td>Percentage of in-scope assets scanned by the City/County-accessible vulnerability scanning platform (authenticated scans where supported) at least weekly.</td><td>95%</td></tr>
<tr><td>5</td><td>Vulnerability Remediation</td><td>Remediation within the patching tier timeframes (Known Exploited: 14 days; Critical: 15 days; High: 30 days; Medium: 90 days), measured from public release.
<table>
<tr><th></th><th>Publicly Exposed?†</th><th>In the KEV?*</th><th>Automatable by Adversary?*</th><th>Technical Impact*</th><th>Agency Timeline (Calendar Days) for Remediation</th></tr>
<tr><td>1</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Total control</td><td>3 days & forensic triage</td></tr>
<tr><td>2</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Partial control</td><td>3 days</td></tr>
<tr><td>3</td><td>Yes</td><td>Yes</td><td>No</td><td>Total control</td><td>3 days & forensic triage</td></tr>
<tr><td>4</td><td>Yes</td><td>Yes</td><td>No</td><td>Partial control</td><td>14 days</td></tr>
<tr><td>5</td><td>Yes</td><td>No</td><td>Yes</td><td>Total control</td><td>3 days</td></tr>
<tr><td>6</td><td>Yes</td><td>No</td><td>Yes</td><td>Partial control</td><td>14 days</td></tr>
<tr><td>7</td><td>Yes</td><td>No</td><td>No</td><td>Total control</td><td>14 days</td></tr>
<tr><td>8</td><td>Yes</td><td>No</td><td>No</td><td>Partial control</td><td>60 days</td></tr>
<tr><td>9</td><td>No</td><td>Yes</td><td>Yes</td><td>Total control</td><td>3 days & forensic triage</td></tr>
<tr><td>10</td><td>No</td><td>Yes</td><td>Yes</td><td>Partial control</td><td>14 days</td></tr>
<tr><td>11</td><td>No</td><td>Yes</td><td>No</td><td>Total control</td><td>14 days</td></tr>
<tr><td>12</td><td>No</td><td>Yes</td><td>No</td><td>Partial control</td><td>14 days</td></tr>
<tr><td>13</td><td>No</td><td>No</td><td>Yes</td><td>Total control</td><td>60 days</td></tr>
<tr><td>14</td><td>No</td><td>No</td><td>Yes</td><td>Partial control</td><td>60 days</td></tr>
<tr><td>15</td><td>No</td><td>No</td><td>No</td><td>Total control</td><td>Fix on system upgrade</td></tr>
<tr><td>16</td><td>No</td><td>No</td><td>No</td><td>Partial control</td><td>Fix on system upgrade</td></tr>
</table></td><td>Per CISA table</td></tr>
<tr><td>6</td><td>Internet Facing Systems (under City/County Mgmt.)</td><td>Critical and Known Exploited vulnerabilities on internet-facing systems remediated or mitigated within CISA guidelines.</td><td>98%</td></tr>
<tr><td>7</td><td>Penetration Testing</td><td>1. Annual external and internal penetration test by an independent third party.
2. Funded by the City/County. Planning and execution are mutually agreed upon.
3. Remedy PLAN for critical findings within 30 days of the PEN report publish.</td><td>City/County Report (100%)</td></tr>
<tr><td></td><td>Security Monitoring & Incident Response</td><td></td><td></td></tr>
<tr><td>8</td><td>Alert Triage</td><td>Security alerts from EDR, SIEM, or other monitoring tools triaged 24x7x365. Critical within 15 minutes of notification. Time stamp from SIEM. Remainder follows Sev 1 SLA guidelines (urgent policy for 24-hour depts)</td><td>95%</td></tr>
<tr><td>9</td><td>Containment</td><td>Affected endpoint or account isolated or disabled within 30 minutes (from receipt of the alert) of a confirmed Critical or High security incident, unless the City/County directs otherwise.</td><td>95%</td></tr>
</table>

	MSA: SECURITY SERVICES	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	SLA
10	Incident Notification	City/County notified by phone and email within 1 hour of detecting a suspected or confirmed security incident, with a preliminary written summary within 24 hours.	Target 100% (each incident)
11	Post-Incident Reporting	Final incident report within 10 business days of containment, covering root cause, timeline, systems and data affected, actions taken, and preventive recommendations. (Part of standard Policy & Procedure activities)	Report (100%)
12	Incident Response Readiness	Incident response plan reviewed and updated annually with the City/County, and at least one tabletop exercise per year involving City/County staff. (Part of standard Policy & Procedure activities)	Report (100%)
	Identity & Privileged Access		
13	MFA Coverage	Multi-factor authentication enforced on all privileged accounts, remote access, and email/cloud applications – Where possible/feasible. (Part of standard Policy & Procedure activities)	Target 100%
14	Privileged Access Review	Quarterly review of all privileged and service accounts, with results reported to the City/County. Unneeded access was removed within 5 business days of the review. (Part of standard Policy & Procedure activities)	Report (100%)
15	Monthly Security Report	EDR coverage, scan coverage, remediation compliance by tier, overdue vulnerabilities (with how long each has been open), active exceptions, security incidents, and alert volume and triage times. (Part of standard Policy & Procedure activities)	Report (100%)

	MSA: CYBER-SECURITY	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	SLA
1	Security Patches	CVE – Critical Same business day	See Vulnerability Remediation Table (SLA #5)
2	Security Patches	CVE – High - DMZ Servers/appliances – Same business day	See Vulnerability Remediation Table (SLA #5
3	Security Patches	CVE – High – Remaining devices	See Vulnerability Remediation Table (SLA #5)
4	Security Patches	CVE – Medium	See Vulnerability

	MSA: CYBER-SECURITY	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	SLA
			Remediation Table (SLA #5)
5	FOB Access Review	Quarterly (Part of standard Policy & Procedure activities)	Report (100%)
6	Block Known IPs	Update rules to block known threat actor IP addresses	Ongoing
7	Dark Web Monitoring	Monitor the dark web for exposed credentials and report when identified. (See also security awareness training in section 3 below) (Part of standard Policy & Procedure activities)	Report (100%)

	MSA: ASSET MANAGEMENT	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
1	Target A: Network attached - Automatic Discovered Data Fields	Includes any/all IMAC activity as well as end of life devices. Of devices capable of being automatically discovered and monitored. Includes tablets/iPads. The C/C will periodically audit all such reported data and discuss any discrepancies with the Service Provider.	98%
2	Target B: Network Attached - Manually Updated Data Fields	Measured daily. Reported quarterly or upon request. Includes any/all IMAC activity as well as end of life devices. Includes tablets/iPads. The C/C will periodically audit all such reported data and discuss any discrepancies with the Service Provider.	90%
3	Target C: Non - Network Attached - manually Updated Data Fields	Measured daily. Reported quarterly or upon request. Includes any/all IMAC activity as well as end of life devices Includes tablets/iPads. The C/C will periodically audit all such reported data and discuss any discrepancies with the Service Provider.	85%
4	Inventory	Physical inventory of all data centers and network closets. (Part of standard Policy & Procedure activities)	100%
5	Inventory – Annual	Annual physical inventory of 20% of IT assets rotating through all offices every 5 years. (Part of standard Policy & Procedure activities) NOTE: Definition of specific items to be included in an "asset record" TBD by the City/County and Service Provider at time of inventory.	100%
6	Capital Assets	All capital assets (as defined by agency) are reconciled with agency capital asset manager	100%

	MSA: ASSET MANAGEMENT	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
7	Licensing	Annual report of all software licenses and corresponding usage by employee per an agreed upon list of City/County applications. (Part of standard Policy & Procedure activities)	Report (100%)
8	Outdated Assets	Maintain a list of hardware/software that is outdated. NOTE: Present C/C with EOS date along with a proposed schedule for retirement. (Part of standard Policy & Procedure activities)	Report (100%)
9	Reporting	Annual (or on demand) list of assets, with their expected replacement date for budgeting. (Part of standard Policy & Procedure activities)	Report (100%)

	MSA: APPLICATION SERVICES	Service Measure / Performance Target					SLAs/XLAs
	Measure	**Description**					**SLA**
1	XLA: Monthly Response Time Impact Analysis	Monthly Report on Applications experiencing response time issues and/or multiple problem tickets for escalation to projects for resolution.					98%
2	Assist 3rd Party Support & Maintenance	Work with 3rd party vendors to provide input and guidance on support and maintenance levels where appropriate and beneficial/value add to the City/County. (Part of standard Policy & Procedure activities)					KPI (100%)
	Sev Level SLAs	**Respond Within**	**SLA**	**Plan Within**	**SLA**	**Resolve Within**	**SLA**
3	**Severity 1—Urgent**	30 min	90%	2 hours	90%	6 hours	**90%**
4	**Severity 2—Critical**	1 hour	90%	3 hours	90%	24 hours	**90%**
5	**Severity 3—Normal**	1 day	90%	1 week	90%	3 weeks	**90%**
6	**Severity 4—Cosmetic**	2 days	90%	1 week	90%	5 weeks	**90%**
	Sev Level Foot Note:	Tickets that require application code changes. Data errors that cause a program to not work should have the data corrected within the normal Severity Level SLA					See Sev Level Table

	MSA: PROJECTS AND PORTFOLIO MGMT	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
1	Project Scoping: Define, scope, and build the plan.	For projects requests originating from C/C IT Leadership (i.e. the Chiefs): Service provider will submit to the City/County a completed SOW, including business case for project, simple definition of success, start date, expected level of effort (hours), cost (if any), milestone completion dates, and a completion date, within TWO (2) business weeks of receipt of a City/County approved project request form (PRF). For project requests originating from C/C depts/agency's directly to Service Provider: Service Provider will be granted	98%

	MSA: PROJECTS AND PORTFOLIO MGMT	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	**SLA**
		one (1) additional week to meet, understand, discuss needs and alternatives and properly scope project request before solutioning.	
2	Project Mgmt.: Work the plan	Upon City/County approval, Service Provider will manage all tools, process, and people (resources) necessary to facilitate the successful completion of said project, as per the agreed upon SOW. Status reports will be provided on a weekly basis. Delays (regardless of responsible party, cause or intent): City/County will be notified within one (1) business day of delay and agreement on mitigation will be requested at next available portfolio meeting.	98%
3	Project Completion/Close out	Upon successful project completion, Service provider will submit an agreed upon project close-out form (PCF) to the City/County for review and record. PCF will minimally include the following: (1) Lessons Learned, (2) Service Provider and C/C specific feedback, (3) Achievement/Alignment with stated project/sow goals, (4) On-time & On-budget comparison (analysis) to initial project scope, budget and plan. (time & budget) (5) Project acceptance/Sign Off	98%

	MSA: IT GOVERNANCE	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	SLA
G1	IT & Cybersecurity Roadmap	Resultant maintains a rolling cybersecurity roadmap aligned to NIST CSF 2.0 (including the Govern function) and the CISA Cybersecurity Performance Goals. Reviewed quarterly with the City, County, and Utilities CIOs and updated with agreed priorities. (Part of standard Policy & Procedure activities)	Report (100%)
G2	Annual Maturity Assessment	MSP facilitates an annual NIST CSF 2.0 current/target profile assessment. Results set roadmap priorities and inform budget requests. (Part of standard Policy & Procedure activities)	Report (100%)
G3	Risk Register & Exceptions	MSP maintains the cyber risk register and documents exception requests with recommended compensating controls. Customer makes risk-acceptance decisions within 30 days of submission. Reviewed quarterly. (Part of standard Policy & Procedure activities)	Report (100%)

	MSA: IT GOVERNANCE	Service Measure / Performance Target	SLAs/XLAs
	Measure	**Description**	SLA
G4	Monthly Security Scorecard	MSP delivers a monthly scorecard covering patch compliance, agent coverage, MFA coverage, SOC escalations and response times, exposed credentials, training completion and phishing simulation results, open risks, with recommended actions. (Part of standard Policy & Procedure activities)	Report (100%)
G5	Customer Governance Responsibilities	Customer chairs the IT governance/steering body; approves policies and standards; prioritizes and funds the roadmap; makes risk-acceptance decisions; approves maintenance windows; sets security awareness training completion requirements and enforces department follow-up; and owns statutory and regulatory reporting (Indiana Office of Technology, CJIS). (Part of standard Policy & Procedure activities)	Standard Policy & Procedure

3 REVISED POLICY & PROCEDURE / NEW INTIATIVES

The following are revised policy & procedure mandates the City/County would like to make an integral part of this amendment. In addition to revised SLAs, the City/County seeks to enhance quality and performance with respect to the following areas.

3.1 CRITICAL CONTACTS & NUMBERS LIST

See Service Desk SLA #17 above in section 2 for further detail. List can/will be reviewed and updated periodically. Minimally annually. List is in no particular order.

#	Title
1	Radio Shop -Technical Director
2	Plant Superintendent
3	911 Communications - Director
4	Property Manager
5	Police Chief
6	Fire Chief
	(Please monitor, review and update annually or sooner if/when needed as people and titles change)

3.2 ANNUAL AWARENESS TRAINING

Annual Awareness Training will be developed and administered by the Service Provider with oversight and content approval provided by the City/County IT Leadership. The goal is to educate and bring about awareness of the ever changing and growing cyber security threats. Participation in this training should be mandatory by all City/County employees on a (minimally) annual basis.

Training Style: If agreeable by all parties, "training" may take the form of classroom style, CBT or if preferred, Online Video Based Training (VBT). VBT's often can include several questions during the course of the video designed to help ensure comprehension, completion and records results to ensure full participation.

Annual Awareness Training Categories: The City/County is interested in having the following categories be part of the Awareness Training Program.

1. Cyber-Security
2. AI Usage & Compliance
3. Artificial Intelligence (AI) Awareness & Training

3.3 NIST AND CISA GUIDLINES

The following table provides guidance related to specific SLAs identified above.

#	Asset Inventory Field	Attribute Benefit	Priority
1	Active/Supported Communication Protocols	Useful for analyzing network traffic. Initially focus on assets that interact with devices outside the IT/OT perimeter or with supervisory control and data acquisition (SCADA) devices over a wide area network, followed by assets that do not.	High
2	Asset Criticality	Enables assets to be managed based on their operational role, safety impact, and/or exposure to risks.	High
3	Asset Number	Unique identifier assigned to the asset by the organization. Put IT, City, County and Utility IDs in different fields. Since some have up to all four	High
4	Asset Role/Type	Useful for understanding context and function of the asset in the network. Common examples of asset type are: ▪ Engineering workstation ▪ Programmable logic controller (PLC) ▪ Historian ▪ Network switch/router ▪ Hypervisor host	High
5	Hostname	Potentially useful for understanding context and function of the asset in the network if included in host naming conventions. (For virtual servers/workstations)	High
6	IP Address(es)	Useful in analyzing network traffic.	High
7	Logging	Provides details about how logs from the asset are collected to enable detection and investigation of potentially malicious activity.	High
8	MAC address(es)	Useful for determining manufacturer, if not otherwise specified. (**Note:** Could only refer to network card manufacturer.)	High
9	Manufacturer	Useful for determining known vulnerabilities.	High
10	Model	Useful for determining known vulnerabilities.	High
11	Operating System	Useful for determining known vulnerabilities, if applicable.	High
12	Physical Location/Address	Provides detail on where to find the asset.	High
13	Ports/Services	Useful for verifying role and determining attack surface, but extremely time consuming to develop and maintain. Initially focus on assets that interact with devices outside the OT security perimeter or with SCADA devices over a wide area network, followed by assets that do not. **Note:** If there is not an active cyber security control (e.g., a firewall) preventing communication outside the OT perimeter, then focus would apply to all assets for ports/services.	High
14	User Accounts	Useful in knowing which user account is expected to be most active, or if the asset is expected to be accessed by many different users.	High
15	Backup Frequency/Type	Provides frequency for how often backups are performed (e.g., daily, weekly, monthly) and method used (e.g., full, incremental, differential).	Medium

16	Baseline Image	Useful to know if there is a particular known-good image that the OS installation was based on, aiding in post-incident recovery.	Medium
17	Department/Owner	Useful in understanding who owns or is responsible for the asset.	Medium
18	Distributor	Useful in understanding where an asset originates (may not be manufacturer).	Medium
19	Firmware/Software Version	Useful for determining known vulnerabilities, if applicable.	Medium
20	OS Version	Useful for determining known vulnerabilities, if applicable.	Medium
21	Physical or Virtual	Provides context on whether asset is physical or virtual.	Medium
22	Virtual Local Area Network (VLAN)	Offers visibility into the asset's network structure.	Medium
23	Antivirus (AV)/Endpoint Protection	Provides details on the asset's capability to protect itself from malicious activities.	Low
24	Date of Manufacture	Useful in determining obsolescence.	Low
25	Hypervisor/VMWare (if applicable)	Provides context in what type of virtualization software is running the virtual machine (VM).	Low
26	Local Time Zone	Useful when conducting user behavior analysis where timelines come into play.	Low
27	Location Within Hypervisor (if applicable)	Provides context on where the VM resides within the hypervisor.	Low
28	Network Monitoring	Provides information about how well communications to the asset are monitored to detect potentially malicious communications.	Low
29	Notes/Description	Provides additional context about the asset, how it is used, issues it has had, etc.	Low
30	Primary Communication Method	Useful to limit attack surfaces and assess whether an incident is local, remote, or network-wide (e.g., wired, wireless, cellular, microwave/radio frequency (RF), satellite), and corollary to communications protocols.	Low
31	Serial Number	Unique identifier; needed to verify some access to vendor patches/support.	Low
32	Time Source	Provides clarity on how an asset synchronizes its operations (e.g., Network Time Protocol (NTP), GPS, Atomic Clock, Local Clock) as disruption of an external time source and associated drift could result in significant impacts.	Low

3.4 ASSETS: HARDWARE, SOFTWARE AND INFRASTRUCTURE DEFINITION

The following Asset definitions are designed to help guide the City/County and Service Provider discussions regarding asset definition and what specifically should be included in the asset record, and ongoing asset management. Mutal agreement will be achieved prior to commencement of asset collection. Additionally, asset definition should be reviewed and trued up on an annual basis to ensure accuracy.

Hardware & Infrastructure Assets (Control 1)

1. Hardware Address: MAC address or unique physical hardware identifier

2. Network Address: IP address (specifically if static)
3. Machine Name: Hostname or fully qualified domain name {FQDN)
4. Asset Owner: The individual responsible for the life cycle and security of the asset
5. Associated Department: The business unit or team using the asset
6. Approval Status: Explicit binary indication of whether the asset has been approved to connect to the network.
7. Asset Environment/ Class: Categorization based on whether it is an end-user device (including mobile), server, network infrastructure device, or non-computing/loT device

Software Assets (Control 2)

1. Software Title & Publisher: Exact commercial name of the installed application or OS
2. Version Number: Current patch or release version number
3. Support Status: Documentation indicating whether the version is actively supported

3.5 DISASTER RECOVERY MANAGEMENT & TESTING

On an annual basis, agreed to by both parties, a Disaster Recovery Plan Meeting/Review will be conducted. Based on the outcomes, goals and agreed upon objectives, a Disaster Recovery Test will be completed annually as well to verify accuracy of the plan and disaster preparedness.

3.6 NEW INTIATIVES: KEEPING CURRENT WITH POLICY AND PROCEDURE

The following initiatives are provided as a roadmap for the City/County and Service Provider to discuss and mutually agree upon details to implement new initiative designed to keep the City/County current and (IT security) safe with advancing technologies in the market.

On a minimal annual basis, new initiatives list will be reviewed and trued up via a simple MSA amendment document.

1. **AI Roadmap:** Define policies/procedures, and an AI roadmap that covers 2027 through 2028 of initiatives to achieve to increase both 1st call resolution and tickets that users were able to resolve on their own. Parties will discuss and agree on a set of initiatives and updated policies/procedures related to an AI roadmap.

2. **HRIS & AD Integration Project:** The City/County agrees to an HRIS and AD integration project so the HRIS platform and AD can accurately work in concert to facilitate a more reasonable and efficient IT and security management process and procedure.

3. **Roadmap:** The City/County and Service Provider should plan to meet quarterly to discuss current and future initiatives to keep current with planned Policy and Procedure. As per the description and intent of this section.

4 PROFESSIONAL FEES

This AMENDMENT is incorporated into and made a part of the Master Services Agreement (MSA) by and between the City/County and Service Provider.

All fees for the Services described within the MSA and this Amendment shall be paid in accordance with this Amendment TWO (2) as per the terms and timeline described within. The City/County shall not be required to pay Service Provider any amounts for the Services other than those set forth under this AMENDMENT and applicable MSA sections.

Professional Fees: TOTALS				
	Past Amendment (2026)	Year ONE (2027)	Year TWO (2028)	Year THREE (2029)
Base Fees	$9,385,570	$9,948,705	$9,849,218	$9,750,725
Formatta (City only)		$85,000	$42,500	$0
Fire Stations (County only)		$160,000	$180,000	$178,200
Project Set Aside Budget	$360,000	$360,000	$360,000	$360,000
TOTAL	**$9,745,570**	**$10,553,705**	**$10,431,718**	**$10,288,925**

Professional Fees: City/County ANNUAL split (Civil City, City Utilities, County) (40%, 20%, 40%)				
	Past Amendment (2026)	Year ONE (2027)	Year TWO (2028)	Year THREE (2029)
Civil City	$3,874,228	$4,184,482	$4,102,187	$4,020,290
City Utilities	$1,997,114	$2,109,741	$2,089,844	$2,070,145
County	$3,874,228	$4,259,482	$4,239,687	$4,198,490
TOTAL	**$9,745,570**	**$10,553,705**	**$10,431,718**	**$10,288,925**

Professional Fees: City/County MONTHLY split (Civil City, City Utilities, County) (40%, 20%, 40%)				
	Past Amendment (2026)	Year ONE (2027)	Year TWO (2028)	Year THREE (2029)
Civil City	$322,852	$348,707	$341,849	$335,024
City Utilities	$166,426	$175,812	$174,154	$172,512
County	$322,852	$354,957	$353,307	$349,874
TOTAL	**$812,131**	**$879,475**	**$869,310**	**$857,410**

5 SIGNATURES

IN WITNESS WHEREOF, the parties hereto have executed this AMENDMENT TWO (2) to the Master Services Agreement (MSA) on the dates prescribed below.

RESULTANT ("Service Provider")

By: _____ Date: _____

Printed: _____

Title: _____

AS SIGNED BY THE CITY OF FORT WAYNE, IN. ("City/County")

By: _____ Date: _____
Pat Roller, City Controller – City of Fort Wayne, IN

AS SIGNED BY THE COUNTY OF ALLEN, IN. ("City/County")

By: _____ Date: _____
Ronald W. Turpin, Commissioner – County of Allen, IN

By: _____ Date: _____
Therese M Brown, Commissioner – County of Allen, IN

By: _____ Date: _____

Richard E. Beck, Commissioner – County of Allen, IN

By: _____ Date: _____

Chris Cloud, Deputy Auditor – County of Allen, IN

APPROVED AS TO FORM AND LEGALITY:

By: _____ Date: _____

Malak Heiny, City Attorney – City of Fort Wayne, IN

By: _____ Date: _____

Laura Maser, County Attorney – Allen County, IN

COUNCIL DIGEST SHEET

Enclosed with this introduction form is a tab sheet and related material from the vendor(s) who submitted bid(s). The Purchasing Department is providing this information to Council as an overview of this award.

RFPs & BIDS

Bid/RFP #	
Awarded To	
Amount	N/A
Conflict of interest on file?	☐ Yes ☐ No
Number of Registrants	N/A
Number of Bidders	
Required Attachments	

EXTENSIONS

Date Last Bid Out	
# Extensions Granted To Date	None

SPECIAL PROCUREMENT

Contract #/ID *(State, Federal, Piggyback--Authority)*	Indiana State Contract #
Sole Source/ Compatibility Justification	

BID CRITERIA *(Take Buy Indiana requirements into consideration.)*

Most Responsible, Responsive Lowest	☐ Yes ☐ No *If no, explain below*
If not lowest, explain	

COUNCIL DIGEST SHEET

COST COMPARISON

Increase/decrease amount from prior years For annual purchase (if available).	

DESCRIPTION OF PROJECT / NEED

Identify need for project & describe project; attach supporting documents as necessary.	Amendment Two extends the joint City/County IT services agreement with Resultant for 2027-2029. Resultant operates, supports and secures the shared technology behind City services, including networks, servers, data centers, backup and disaster recovery, cybersecurity, computers and mobile devices, business and GIS applications, help desk and project management. The amendment adds a dedicated cybersecurity program with 24/7 monitoring and response, 24-hour support provided directly by Resultant staff, mobile device management, and measurable performance standards with regular reporting and audit rights.

REQUEST FOR PRIOR APPROVAL

Provide justification if prior approval is being requested.	N/A

FUNDING SOURCE

Account Information.	
	Fund Dept Org Object = 00022603-5314 and 95045063-5369

Fort Wayne City Council
c/o City Clerk' Office
Fort Wayne, IN 46802

Subject: IT Services – Resultant Master Services Agreement, Amendment Two (2027–2029)

Members of City Council:

This ordinance authorizes the purchase of Computer Services from Resultant for 2027-2029. It is the second extension of the original contract signed in 2021. We will issue an RFP for services to start in 2030.

Resultant operates, supports and protects the technology behind nearly every service the City delivers: the networks, servers and data centers that keep systems running; backup and disaster recovery; cybersecurity; the computers and mobile devices our employees use; the business and GIS applications departments use to serve residents; and project management for the City's technology initiatives. Many of the departments supported never close, including 911, police, fire, the radio shop, maintenance departments and our water filtration and water pollution control plants.

Cybersecurity is a central focus of this amendment. Local governments are frequent targets of ransomware and other attacks, and the threats change constantly. Amendment Two builds upon an already robust cybersecurity program so that the City keeps pace with the latest threats, including:

- Around-the-clock monitoring of City systems, with rapid response
- Ongoing vulnerability management to find and fix weaknesses before they can be exploited
- Cybersecurity awareness training for City employees
- Monitoring for stolen or exposed employee credentials
- Annual independent penetration testing and annual incident response and disaster recovery exercises
- Alignment with national cybersecurity guidance from NIST and CISA
- Support for the City's legal obligation to report cybersecurity incidents to the Indiana Office of Technology within 48 hours

Resultant has been key to the modernization and hardening of our infrastructure. Key goals of the next 3 years are:

- Maturing our cybersecurity program in line with national standards
- Migrating some of our custom applications to our larger platforms
- Updating code for those applications that can't be migrated
- Migration of electronic forms to CivicPlus
- Creating a governance structure for risk assessment and IT projects
- Creating an AI roadmap and implementing approved projects

If you have any questions, please contact us.

Bob Thiele
CIO
City of Fort Wayne
260-427-1400

Joe Welch
CIO
City Utilities
260-427-5561