STATEMENT OF WORK
RAVENII MANAGED SECURITY & SOC SERVICES & VCISO ADVISORY PROGRAM

This Statement of Work (this "SOW"), under the Master Services Agreement between the City of Joplin, a Missouri municipality ("Customer") and RAVENi, L.L.C., a Missouri limited liability company ("RAVEN") dated **06/01/2025** (the "Agreement") is entered into as of the SOW Effective Date set forth below. The terms and conditions of the Agreement are hereby incorporated herein by reference. In the event of a conflict between the Agreement and the SOW, the terms of the Agreement shall prevail, unless the SOW expressly references the specific provision in the Agreement to be modified by the SOW. Al capitalized terms that are used but not defined in this SOW shall have the respective meanings given to them in the Agreement.

1. SOW Term. The term of this SOW shall begin effective as of the following SOW Effective Date: June 1, 2025

The SOW this Agreement shall commence on the Effective Date and continue for an initial period of three (3) years (the "Initial Term"), unless earlier terminated in accordance with the provisions herein. Upon expiration of the Initial Term, Client shall have the option to renew this Agreement for up to two (2) additional one-year periods (each, a "Renewal Term"), by providing written notice to Service Provider at least thirty (30) days prior to the expiration of the Initial Term or then-current Renewal Term. The Initial Term and any Renewal Term(s) shall collectively be referred to as the "Term." The terms and conditions of this Agreement shall apply throughout any Renewal Term, unless otherwise agreed to in writing by both parties.

Customer may terminate this SOW prior to the end of the three-year term, upon thirty (30) days written notice to RAVENii and payment by Customer to RAVENii an early termination fee in the amount of ½ the remaining contractual amount. Customer may change the initial Tier structure upon thirty (30) days written notice to RAVENii.

2. Description of Services. RAVENii shall perform the following Services, and any other services as may be requested from time to time, including modifications to the Services set forth herein, in accordance with the terms and conditions set forth in the Agreement and in this SOW:

RAVENii's SOC as a Service
RAVENii's SOC as a Service (SOCaaS) delivers powerful threat detection, incident response, and compliance management in one fully managed service. We combine all the security capabilities needed for effective security monitoring across your cloud and on-premise environments like:

- Asset discovery
- Continuous Internal and External Vulnerability management
- Intrusion detection
- Endpoint detection and response
- Behavioral monitoring
- SIEM log management
- Compliance reports

RAVENii's Managed SOC provides:

- 24x7 monitoring

- System alerts
- Security alerts
- Prioritization of risks
- Remediation recommendations
- Troubleshooting
- 24x7 dashboard access for reporting
- Monthly executive briefings with RAVENii SOC subject matter experts
- RAVENii C-Level access and support
- Dedicated account & project manager for onboarding and account maintenance
- Co-managed, shared dashboards

RAVENii's Managed Endpoint Protection

The RAVENii Managed Endpoint Protection Service helps businesses block threats and other attempts to gain access into their networks. RAVENii will defend all access points with 24/7 monitoring for any malicious activity.

The service follows security best practices and ensures that the endpoints of security; the client devices, are protected against advanced threats, keeping networks running and corporate assets safe. With RAVENii's Managed Endpoint Protection Service you can protect your intellectual property, customer data, and reputation. You can also devote more IT resources to your core business.

RAVENii's Managed Endpoint Protection Service includes:

Malware Protection
Internet Filtering
Device lockdown, alarming and wiping
Device Tracking and Reclamation
Daily Asset Inventory of hardware and software
Microsoft OS patching
3rd Party Application patching
24x7 monitoring
24x7 Event Log Collection
Daily backup of folders or entire systems
Regular executive indicator and reporting debriefs
Access to RAVENii's Security Incident Response and Management Team
Anytime/Anywhere management of endpoints

RAVENii will provide 24x7 Management and Monitoring of the City's endpoint protection software for all endpoints within the City's scope.

RAVENii will:

- Notify customer of security issues identified for all endpoints/devices in scope;*
- Provide remediation of security issues identified for all endpoints/devices in scope;*
- Provide a Root Cause Analysis of security issues identified for all endpoints/devices. The RCA will outline the details of discovery and remediation for issues related to endpoints/devices;
- Review and recommend updates to agents, and support for agent and console issues related;
- Open and manage Support issues related to the functionality of subscribed endpoint protection products on behalf of the customer until resolution.

- Other (Out of Scope) Services will be mutually agreed upon. Incident Response is considered Out of Scope on any Customer endpoint/device that the Customer creates exceptions or deviations to the configuration guidelines for the endpoint protection product.

* Everything related to a virus being detected by the endpoint protection product managed by RAVENii is in scope. The definition of an In Scope incident is something that is detected by RAVENii on an endpoint/device with their endpoint protection product deployed on it in the Customer's environment that requires remediation action. RAVENii will quarantine, contain, or clear any endpoint/device as long as RAVENii has access to the endpoint/device.

RAVENii's Network Security Monitoring

RAVENii offers 24X7 Network Security Monitoring of your network and strongly recommends deploying this solution in your environment. Our platform utilizes context-aware AI, a dynamic network baselining technology which allows us to identify pre-attack behavior and stop attacks before they happen.

A full baseline of your typical network behavior can be created in just 7 days. This allows us to see your entire attack surface. Having this greater transparency allows for faster detections, better correlation, and less noise so you can focus on what matters. The AI functionality eliminates 95% of the false positive alerts that typically send IT teams down the wrong track. The value to you is real and actionable threats to focus on, not distractions and wild goose chases.

RAVENii will monitor all of your network traffic, incoming, outgoing, and local in the cloud, on premise, or in hybrid environments. With full layer 2-7 visibility, full packet capture, and deep packet inspection, we can give you the visibility you need to see and take action before damage is done.

RAVENii will enhance your security by doing the following:

- Establishing an evolving baseline of acceptable network behavior for anomaly detection in 7 days or less, without requiring months of historical data, human intelligence or forensics;
- Providing predictive and "zero day" threat, attack, and anomaly intelligence layer without human intervention; and
- Delivering an average of 95% reduction in false positive alerts.

RAVENii's Network Security Monitoring Service Includes …

- Malware detection with built-in threat intelligence;
- Real-time attack surface measuring;
- Real-time on-the-wire passive vulnerability assessment and threat monitoring;
- Real-time indicator of compromise alerting;
- Real-time detection of botnet and command & control traffic;
- Forensics;
- Trending Data;
- Access to RAVENii's Security Incident Response and Management Team; and
- Access to RAVENii's web based SOC for managed devices, workflows, alerting and incidents.

RAVENii's External Penetration Test & Quarterly Scans

RAVENii's Certified Ethical Hackers will perform External Network Penetration Tests to discover, actively exploit, and report vulnerabilities to the City about the health of its network environment.

RAVENii has adopted a methodology based on guidance provided by the Penetration Testing Execution Standard (PTES, www.pentest-standard.org). Penetration tests are conducted following this methodology and documentation, where applicable, and will be conducted to support the findings contained in the report.

RAVENii's Managed Security Awareness & Phishing Training

RAVENii will provide the Managed Security Awareness Training licensing and manage the training platform for the City of Joplin. This service follows best practices for educating your human firewall on how to treat your sensitive data and be security aware. Management of your Security Awareness Training platform will include:

- Ongoing security awareness training & testing to ensure the Customer's employees understand and exhibit the necessary behaviors and skills to help protect the security of the organization.
- Coordination with Customer's Security & Compliance Teams to ensure training meets the Customer's business requirements.
- Training to all City employees and Council members on how to utilize secure authentication, how to identify social engineering attacks, how to identify and properly manage sensitive data, how to identify causes for unintentional data loss, how to identify the most common indicators of an incident, etc.
- Remediation plans for repeat offenders.
- Campaign and status reports.

The Managed Security Awareness Training platform also includes:

- Initial Onboarding
- New Hire Onboarding
- Offboarding
- User Management & Support
- Phishing Campaigns (up to 12 per year)
- Full access to content library, including Compliance training modules

RAVENii's Firewall IPS/IDS with 24/7 Monitoring

RAVENii will monitor the City of Joplin's firewalls 24/7 and provide daily alerting and weekly/monthly reporting.

RAVENii will monitor the firewalls daily for uptime, usage, and overall health of the system interface.

RAVENii will perform ongoing firewall traffic analysis.

RAVENii will monitor the firewall manufacturer's site for system updates/upgrades, provide a summary of the possible effects, and will seek approval from the City before proceeding with the work.

RAVENii will provide technical analysis of the firewall systems to ensure the City is leveraging the best practice functionalities of the tool for security purposes.

RAVENii will provide a Best Practice Assessment for newly acquired firewall assets as they are integrated into the City's network.

RAVENii will provide a Best Practice Assessment for all firewall assets on an annual basis.

RAVENii's Backup Management Solution

The following details define RAVENii's Backup Service that we recommend for the City of Joplin:

- Service provided utilizing Syxsense
- Centralized management console
- Agent based
- Full back up with differentials to follow
- Cloud & Local backups
- File based backups & restores
- Image based backups & restores
- Office 365 mailbox backups
- Individual email restores
- Customized scheduling
- Customized retention policy & restore times
- Local Backups per device as required

*NAS/SAN for local backups must be provided by customer

RAVENii will initiate restore requests within 4 business hours from the receipt of the request. Restore requests will be done during regular business hours: Monday through Friday from 8 am – 5 pm. Restore time is dependent upon the amount of data to be restored.

All data restore requests should be submitted to RAVENii via a support ticket through our web-based service desk.

RAVENii's vCISO Advisory Program

The City of Joplin has requested recommendations for tools and/or security best practices to follow in this RFP. RAVENii always recommends our vCISO Advisory Program to anyone interested in building or fortifying a security program. We recommend it to anyone wanting a thorough audit of your current state of security as well as for strategizing and building a roadmap for your end state goal.

RAVENii believes a complete and sound security program consists of policies and procedures that govern the use of security tools. RAVENii's vCISO program is a 12-month advisory service designed to evaluate your current security footprint, expose your security vulnerabilities, create a full set of security policies, and facilitate a plan of action to continually be improving your security posture.

RAVENii's vCISO program follows the Top 18 CIS Controls, a set of prioritized security actions that aid in finding ways to stopping today's most dangerous attacks. The 18 Controls cover most cyber-attack vectors and takes leading threat data from forensic experts across all industries and transforms it into actionable controls to achieve a better overall cybersecurity defense.

RAVENii's vCISO program will:

- Evaluate, create, and direct an Information Security Program Plan for the City of Joplin;

- Itemize, catalogue, evaluate and, as necessary, further develop your Information Security Policies and Procedures;
- Identify and confirm your vulnerabilities to information systems from internal and external threats by auditing the current architectures and system configurations;
- Itemize, quantify, and rank your information security risks, based upon the potential impacts to the organization;
- Minimize or eliminate business risks and exposures by identifying short- and long-term options and solutions for remediation of identified vulnerabilities;
- Determine the appropriate approach to develop or improve upon your existing Information Security program;
- Establish and/or evaluate Security Policies & Procedures to govern the security of your network, data, and applications;
- Ensure that security programs are in compliance with applicable laws, regulations, and policies to minimize or eliminate risk and audit findings;
- Develop an incident response plan with key staff, including incident response plan documentation developed specifically for your existing infrastructure; and
- Assist the City in determining and mitigating third party vulnerabilities.

Four (4) hours per month of vCISO level consulting activities. Example activities include, but are not limited to the following:

Identification of priority action items to close gaps quickly
Strategic Roadmaps with Level of Effort (LOE)
Maturity modeling gaps to help show business context
Network infrastructure segmentation & architecture planning
Creation of Incident Response Plan & Communications Plan
Table Top testing for Incident Response
Security Policy & Process Creation
Security Tools Assessment
Security Program Evaluation
Security Program Development
SOC2 Audit Preparation Assistance
Vendor Management Program
Regulatory and Compliance Issues
Critical Security Controls
Map to CJIS Controls

Other (Out of Scope) Services

- All incident response is considered out of scope and will be billed at $400/hour.

3. List of Deliverables. RAVENii will provide the following deliverables to the City:
   - Endpoint Security - Managed Endpoint Protection as listed above
   - Server and Workstation Security
   - Network Protection - Managed Endpoint as listed above.
     - Daily Health Checks
     - Weekly Operational Reporting
     - Monthly Executive Reporting

- Network Protection as listed above.
    - Daily Health Checks
    - Weekly Operational Reporting
    - Monthly Executive Reporting
- Daily Health & Safety Checks
- Weekly Reporting
- 24/7 Monitoring
- Quarterly Assessment - External Penetration Test with Quarterly External Scans as above.
    - This report outlines any exceptions identified during the external penetration testing periods as well as recommendations to mitigate those risks.
- Annual Cybersecurity Training (Onsite)
    - Managed Security Awareness Training as listed above.
    - Level 1 & 2 Support* (RAVENii will serve as the escalation path for Level 3 Support with Managed Security Awareness Training)
    - Monthly Executive Report
    - Mapped to Critical Security Controls (vCISO clients)
- Annual Penetration Testing & periodic Phishing & email Security tests
- Firewall IPS/IDS with 24/7 Monitoring as listed above.
    - Daily Health Checks
    - Weekly Operational Reporting
    - Monthly Executive Reporting
- Long-Term Network Advisement and Infrastructure Enhancement
- Incident Response plan & preparation
- Air Gap Backup & Recovery - Managed Backup services as listed above.
    - Daily Health Checks
    - Weekly Operational Reporting
    - Monthly Executive Reporting
- SOCaaS as listed above.
    - Daily Health Checks
    - Weekly Operational Reporting
    - Monthly Executive Reporting
- vCISO Advisory Service as listed above.
    - Compliance Framework Assessments, Analysis, and Mapped to CJIS.
- Web-based Service Desk to open tickets, track workflows, manage devices, alerting and incidents.
- Reporting as needed for business or compliance requirements.

4. Acceptance and Testing.
5. Service Fees. Customer shall pay RAVENii the fees and expenses set forth below.

Service Description	Fee/Price	Frequency
Endpoint Security	Managed Endpoint Protection | 550 Endpoints	

Server and Workstation Security	Network Security Monitoring/Managed Endpoint Protection	
Network Protection	Network Security Monitoring | 500 Mbps	
Daily Health & Safety Checks	SOCaaS	
Weekly Reporting	SOCaaS	
24/7 Monitoring	SOCaaS	
Quarterly Assessment	External Penetration Test & Quarterly Scans | 4 Tests | sub 256 IPs	
Annual Cyber-Security Training	Security Awareness Training | 550 Users	
Annual Penetration Testing & Periodic Phishing & Email Security Tests	External Penetration Test & Quarterly Scans / Managed Security Awareness Training	
Firewall IPS/IDS with 24/7 Monitoring	Firewall Monitoring	
Long-term Network Advisement and Infrastructure Enhancement	vCISO Advisory Program	
Incident Response Plan & Preparation	vCISO Advisory Program	
Air Gap Backup & Recovery	Managed Backup Solution | 100 Devices	
SOC for CyberSecurity	vCISO Advisory Program	
TOTAL		**$19,693.56 / Month**

**Pricing is based on RAVENii providing licensing, hardware where applicable and monitoring. Pricing is also based off utilization (user, IP, bandwidth, device, etc.). If the City exceeds utilization, RAVENii will work with you to right size the environment or add more resources before charging any overage fees. Special configurations for departmental needs may increase cost. See rate card below.*

RAVENii rate schedule for services beyond the scope of activities as listed in this proposal:

- Monday – Friday, 8am-5pm: $250/hour
- Incident Response: $400/hour

6. Work Location / Resources / Facilities. Except as set forth below or as otherwise agreed, RAVENii will perform the Services remotely and will provide all facilities, personnel, equipment, software, hardware and other resources necessary to provide the Service.

   To the extent Customer is required to provide equipment under this SOW, Customer hereby grants to RAVENii, solely for the purpose of performing the Services, the right to access and use such Customer-owned/leased equipment to provide the Services and RAVENii shall be responsible for damage to Customer's facilities, Customer's equipment or other property from such use.

7. Project Management; Contact Information. Individuals will be designated as project managers for the respective parties in the RAVENii onboarding document that will be provided and filled out jointly by Customer and RAVENii.

8. Computer system access. RAVENii personnel will require access to Customer's computer systems/Network environment in order to perform this Service.

9. Additional Terms Applicable to this SOW.

9.1 General. Subject to the terms and conditions of this Agreement, during the Term, RAVENii and its subcontractors shall provide to Client the Services set forth in the applicable SOW.

9.2 SOW Changes. Modifications to Services in a SOW shall be set forth in writing, identifying any changes to the fees and time schedule associated with the modification and such modifications shall be implemented only upon a mutual written agreement of the parties. Additional onboarding fees may apply.

9.3 Reliance. Unless specified otherwise in any SOW, RAVENii and its subcontractors shall be entitled to rely, without verification or investigation, upon any and all instructions, guidelines, information or materials provided or made available by Client.

9.4 Method of Performing Services. RAVENii and its subcontractors, in conjunction with its personnel, will determine the method, details, and means of performing Services for Client. Client acknowledges and understands that the Services may include simulated, attempted and/or actual security breaches to Client’s computer system.

9.5 Non-Exclusivity. Nothing in this Agreement shall be construed or interpreted so as to prohibit RAVENii and its subcontractors from entering into similar agreements with other parties concerning similar Services.

9.6 Maintenance Updates. From time to time, RAVENii and its subcontractors may provide Client with a maintenance update to any of the Services. All warranties, indemnification obligations and duties of RAVENii and its subcontractors are conditioned upon Client’s acceptance and installation of all maintenance updates supplied by RAVENii and its subcontractors.

IN WITNESS WHEREOF, the parties hereto have entered this SOW as of SOW Effective Date set forth above.

By: RAVENII, L.L.C.

Name: Zachary L. Yelland

Title: Operations Manager

Signature: _____

By: City of Joplin

Name: _____

Title: _____

Signature: _____