CITY OF MOAB

REQUEST FOR PROPOSALS

Information Technology Security (Cyber Security) and Information Technology Support Services

March 2026

City of Moab

217 East Center Street

Moab, Utah 84532

(435) 259-5121

CONTENTS

PROPOSALS SUBMITTAL DEADLINE

TUESDAY, APRIL 28, 2026, 2:00 P.M. MDT

INTERVIEWS FOR SELECTED CONSULTANTS

The City of Moab ("City") hereby invites interested individuals and companies to submit written proposals in accordance with the terms, conditions and specifications contained in this document.

GENERAL SCOPE OF SERVICE REQUESTED

The City is requesting proposals from technology consulting firms for Cyber Security and Technology Support Services. The City intends to contract with a qualified firm(s) to provide consultation and guidance for Cyber Security and IT support in the following areas: architectural guidance, project management, technology roadmap, technical implementation, support services and future City technology needs and solutions with an emphasis on technology (cyber) security. Firms may express interest and request consideration for said project by making submittal to the City as outlined herein.

STATEMENT OF PURPOSE - MANAGED INFRASTRUCTURE AND NETWORK SERVICES

the City is seeking comprehensive managed infrastructure and network services. The winning vendor will provide hardware (server, desktop/laptop), network, and software support and monitoring, helpdesk, back-ups, remote access, on-site support, email maintenance and support, inventory control and management (hardware and software), security, and disaster recovery. To accomplish this, it is expected that the winning vendor(s) will be able to work effectively with other the City vendors (such as proprietary software vendors and internet service providers) to make the IT System a seamless process to the end user.

Additional consulting areas include voice and data network, physical security, SCADA security, virtualization, data storage, Windows server, AI governance, and other general infrastructure technologies.

It is also expected that the winning vendor(s) will assist management with long-term planning to keep systems current and functional in the most cost-effective manner possible. Additionally, they will work with the City's IT Supervisor and Technician utilizing already established day-to-day tracking and prioritization system for work order requests from the various departments.

The overall goal of this RFP is to procure long-term, comprehensive, reliable, timely, proactive IT management, cybersecurity and support that will promote the mission of the City in serving its citizens.

MOAB CITY COMMUNITY PROFILE

The City is located just south of the Colorado River in Grand County and is a regional center of southeastern Utah. It is located on the west side of the 12,500-foot-high La Sal Mountains in a valley fifteen miles long and three miles wide within the heart of the Colorado Plateau known as Spanish Valley.

Moab's historical economy was based on farming, ranching, and fruit growing although some mining was done along the Colorado River and in the La Sal Mountains. Moab's largest industry for the last quarter century has been tourism.

The 2020 Census shows the city's current population at 5,369. Jeeping, hiking, climbing, mountain biking and river activities are all recreational opportunities available in Moab.

A five-member City Council and a Mayor govern the City of Moab, whom residents elect for four-year terms. The Mayor acts as the chairperson for City Council meetings, breaks ties, signs official documents, and appoints officials. The City Council approves resolutions, ordinances, and financial activities of the City. The City Council also hires a City Manager, who is the chief executive and who manages all employees of the City.

MOAB CITY TECHNOLOGY PROFILE

A. City Government Network:
   The City Government provides voice and data services to approximately 200 employees in eight departments and fifteen divisions across multiple buildings, including City Hall, Public Works, Wastewater Treatment, Animal Shelter, and the Moab Arts & Recreation Center (MARC).
B. Server and Virtualization Infrastructure: The City has migrated to a virtualized environment utilizing Microsoft Hyper-V.
   1. Physical Hosts: Two (2) Dell PowerEdge R6515 Hypervisors running Windows Server 2019 Datacenter.
   2. Virtual Machines: Approximately 16 virtual servers running primarily Windows Server 2019 Datacenter. Critical workloads include Domain Controllers, File Servers, Print Servers, SQL Servers (Pelorus/Fatpot), and Application Servers (HVAC, 3CX).
   3. Legacy Systems: One legacy VM running Windows Server 2012 R2 (Fatpot - legacy PD) and one isolated VM running Windows 7 (HVAC control).
C. Storage & Backups:
   1. Primary Storage: Synology Flash Cluster SAN (RS3617xs+) and Synology iSCSI Failover SAN (RS2818RP+).
   2. Backup Strategy: Axcient x360 Recover provides image-based backups with offsite replication. Synology DiskStations (DS1621+) supports local backups.
D. Workstations & Laptops: The City supports a mixed fleet of approximately 180+ managed endpoints.

1. Operating Systems: Primarily Windows 11 Pro.
2. Hardware Standard: Diverse environment including Dell Latitude Rugged laptops (Police Department), HP EliteDesk/ProDesk desktops, Lenovo ThinkPads, and Microsoft Surface devices.

E. Network & Security:
    1. Firewalls: SonicWall NSA series (Primary at City Hall) and SonicWall TZ series at remote sites (Aquatics, Animal Shelter, Public Works, MARC).
    2. Switching: Ubiquiti EdgeSwitch and UniFi Pro PoE switches utilized for core and edge networking.
    3. Wireless: Hybrid environment utilizing Cisco Meraki and Ubiquiti UniFi access points for secure internal and public Wi-Fi access.
    4. Remote Access: NetMotion (Absolute Secure Access) for the Police Department and VPN L2TP for other remote users.
    5. Antivirus
F. Phone System:
    1. VoIP Solution: 3CX Phone System (Virtual Machine) utilizing Nuso SIP Trunks.
    2. Hardware: Yealink T46S and T54W handsets deployed across all departments.
G. SCADA Network: The SCADA network monitors the City's municipal water and reclamation facilities.
    1. Infrastructure: FortiNet firewalls managed by third party (Dorsett) with specific VMs (InfoScan) isolated on the City network for monitoring.
H. Enterprise & Departmental Applications:
    1. Productivity: Google Workspace (primary Email/Collab) and Microsoft Office 365 (Desktop Apps).
    2. Financial/HR: Pelorus DGS & Timekeeper (On-premise SQL).
    3. Public Safety: Spillman (hosted by Grand County), Fatpot (Legacy/Maintenance mode), Axon Evidence (Cloud), and NetMotion for secure cruiser connectivity.
    4. Other Critical Apps: Sportsman (Cloud/Web-based for Rec Center), ArcGIS (Engineering), and Ascent Compass (HVAC).
I. Physical Security:
    1. Access Control: Axis A1001 Network Door Controllers managing approximately 29 doors across City facilities. Replacing with Unifi Access Control Units.
    2. Surveillance: ExacqVision NVRs (PD Interview rooms) and Lorex/UniFi camera systems at various facilities.

PART 1 - SCOPE OF SERVICES / PROPOSAL REQUIREMENTS – CYBER SECURITY

The Scope of Services for this RFP is to maintain a robust, proactive IT Security Program. The selected vendor must provide a multi-layered security approach ("Defense in Depth") to ensure the confidentiality, integrity, and availability of the City of Moab's data. The solution must meet Compliance-level standards.

Specific Requirements:

The proposal must demonstrate the ability to provide the following security services:

A. 24/7 Security Operations Center (SOC): Provide continuous 24/7/365 monitoring and response of the City's network environment by a staffed SOC.
B. SIEM & Log Analysis: Deployment of Security Information and Event Management (SIEM) tools to aggregate and analyze event logs from firewalls, servers, and endpoints to identify anomalies in real-time.
C. Advanced Endpoint Protection (EDR): Deployment and management of NextGen Antivirus (NGAV) combined with Endpoint Detection and Response (EDR) software to detect, isolate, and remediate advanced threats (e.g., ransomware, zero-day attacks) that traditional antivirus cannot catch.
D. Protective DNS & Content Filtering:
   Implementation of a Protective DNS solution (e.g., Cisco Umbrella or equivalent) to block malicious domain requests at the DNS layer before a connection is established. The solution must include:
   1. Threat Protection: Automatic blocking of known malware, ransomware, phishing, and Command & Control (C2) callback domains.
   2. Roaming Protection: Agents installed on City laptops to enforce security policies even when devices are off the City network (e.g., employees working from home or hotels).
   3. Content Policy Enforcement: Granular filtering capabilities to block specific categories (e.g., Adult Content, Gambling) in accordance with City HR policies.
E. Managed Intrusion Detection (IDS): Continual monitoring of internal and public-facing infrastructure for intrusion attempts.
F. Vulnerability Management: Continuous vulnerability scanning of the City's IT infrastructure to identify and prioritize risks for remediation.
G. Automated Patch Management: Management of security patches for Microsoft Operating Systems and critical 3rd Party Applications (e.g., Adobe, Chrome, Zoom) to close security gaps.
H. Dark Web Monitoring: Continuous monitoring of the Dark Web for compromised City credentials (emails/passwords) to prevent unauthorized access.
I. Cloud Security & Backup:

1. Configuration and security monitoring of Google Workspaces and Microsoft Office 365 tenants.
2. Automated, immutable backups for Google Workspaces and Office 365 (Exchange, SharePoint, OneDrive) to protect against data loss in the cloud.
3. Server Business Continuity (BCDR):
    i. Image-Based Backups: Deployment of a BCDR solution for all critical physical and virtual servers (as listed in the Technology Profile). Backups must capture the full server state (OS, Apps, Files), not just files.
    ii. Hybrid Storage: Backups must be stored on a local appliance for rapid restoration and replicated to a secure, compliant cloud repository for disaster recovery.
    iii. Instant Virtualization: The solution must demonstrate the ability to "spin up" (boot) servers as virtual machines directly on the local backup appliance or in the cloud to minimize downtime during a hardware failure or ransomware event.
    iv. Automated Verification: Daily automated integrity checks (e.g., screenshot verification) to prove backups are bootable and viable.

J. Security Awareness Training: Provision of an ongoing Security Awareness Training platform for City employees, including automated phishing simulations to test and educate staff.
K. SCADA & Perimeter Security:
    1. Configuration of perimeter security controls (Firewalls/VPNs).
    2. Third party interface with vendor who manages the SCADA system, is limited to access to network through VPN.
    3. Maintain segregation of the City's SCADA network (Water/Reclamation) to ensure isolation from the corporate network.
L. Council Room Audio Visual System:
    1. End User Support: Provide technical assistance to designated City staff to ensure the enable recording, live streaming, and hybrid participation (e.g., Zoom/YouTube) of Council meetings.
    2. Vendor Liaison: Act as the primary technical point of contact with the specialized A/V integrator to troubleshoot hardware or configuration issues with the control systems.
M. Incident Response & Breach Management:
    1. Define, create, and execute on a standard Incident Response Plan (IRP) for phishing, malware, and data breaches.
N. Compliance & Reporting: Real-time visibility into the security posture of the network, including blocked threats, patch status, and vulnerability scores.

PART 2 - SCOPE OF SERVICES / PROPOSAL REQUIREMENTS - INFORMATION TECHNOLOGY SUPPORT SERVICES

The City requires a proactive Managed Services Provider (MSP) rather than a reactive break/fix vendor. The Consultant(s) will provide IT Infrastructure Consulting Services including architectural guidance, technology roadmap insight, technical implementation, support, and project management related to the following specific areas:

Specific Requirements:

The proposal must demonstrate the ability to provide the following support services:

A. Infrastructure & Server Management:
    1. Management and monitoring of the City's hybrid cloud infrastructure, including on-premise Microsoft Hyper-V clusters (Windows Server 2019/2022) and cloud tenants.
    2. Administration of Active Directory, Group Policy, and Azure AD Sync.
    3. Management of Storage Area Networks (SAN) and iSCSI targets (specifically Synology infrastructure) to ensure high availability.
B. Network & Connectivity:
    1. Administration of a complex multi-site Wide Area Network (WAN) across 8+ locations.
    2. Management of VLAN segmentation to ensure security and traffic prioritization (e.g., Voice, Data, Guest, SCADA, and CJIS-compliant Public Safety networks).
    3. Support for Firewall infrastructure (SonicWall) and Switching infrastructure (Ubiquiti/Cisco).
    4. Management of wireless networks including Ubiquiti and Cisco Meraki cloud controllers.
C. Remote End-User & Application Support:
    1. Service Desk: 24/7/365 Help Desk support for Windows endpoints.
    2. Vendor Liaison Services: Acting as the technical point of contact for mission-critical third-party municipal applications. This includes troubleshooting connectivity and facilitating support with vendors for:
        i. Public Safety: Spillman, Fatpot, Axon Evidence (Must understand CJIS compliance).
        ii. Utilities/Finance: Pelorus, Sportsman.
        iii. Facilities: SCADA, Dorsett Controls, and HVAC systems.
        iv. Council Chambers: AV System
    3. SaaS Management: Administration of Google Workspace (G-Suite) and Microsoft Office 365 tenants, including user lifecycle management (onboarding/offboarding).

O. DEDICATED ONSITE STAFFING (STAFF AUGMENTATION):
The City requires a dedicated onsite IT presence to serve as the Primary Tier 1 & Tier 2 Support for City staff. This role is intended to resolve the majority of end-user tickets in-person, utilizing the remote support team only for support of any absences, Tier 3 escalation, project engineering requests, or complex backend issues.

4. Staffing Requirements:
    i. Hours: Provision of a dedicated technician onsite at City Hall for 40 hours per week (e.g., M-F, 8:00 AM – 5:00 PM), plus any overtime as needed.
    ii. Role: This resource will act as the "Face of IT" for the City, handling:
        a. Immediate Response: Instant troubleshooting for Police Department critical issues (MDTs, vehicle connectivity) and walk-up requests.
        b. Physical Logistics: Deployment of new hardware, cable management, and asset retrieval for termed employees.
        c. Vendor Escort: Supervising third-party access (ISP, HVAC, SCADA) to secure areas.
        d. Meeting Support: Hands-on setup for City Council meetings (adjusting schedules to accommodate evening meetings as needed).

D. Voice & Physical Security Support:
1. Maintenance and support of the City's VoIP Phone System (3CX hosted on Hyper-V), including SIP trunk management (Nuso) and handset configuration.
2. Underlying network support for physical security systems, including Axis Door Controllers, Unifi Door Controllers, and IP Camera NVRs (ExacqVision/Lorex).

E. Strategic Planning:
1. Provide a dedicated resource to assist with budgeting, lifecycle management, and long-term technology roadmaps.
2. Strategic Business Reviews: Conduct regular reviews to discuss system health, ticket trends, and future projects.

P. Professional Services:
1. Capability must be displayed by having and executing Information Technology-related projects with best-practice systems via a formal project management structure or equivalent, such as a Project Management Office (PMO).

2. A formal leadership structure of professionally appropriate project management-based leaders should exist. Project Management Professional (PMP), or equivalent, credentials are strongly preferred.
3. Formal systems to manage project schedule and costs should be utilized and issues communicated via a standard cadence. Project scoping should be provided via best practice in formal Statement of Work (SOW) documents.
4. Project-related tasks should be executed as normal course of action such as kick-offs, cutover planning, service hand-off and change control efforts.

PART 3 - SCOPE OF SERVICES – ARTIFICIAL INTELLIGENCE GOVERNANCE & STRATEGY

The City recognizes the growing impact of Artificial Intelligence (AI) on municipal operations and the risks associated with unmanaged AI usage. The selected vendor must provide tools and consulting services to help the City harness AI efficiency while protecting sensitive data (CJIS, PII, and HIPAA).

Specific Requirements:

The proposal must demonstrate capability in the following areas:

A. AI Visibility & Assessment:
    1. Ability to conduct technical assessments to identify unmanaged AI (unauthorized use of public AI tools like ChatGPT) within the City network.
    2. Provide reporting on which employees are using AI tools and the potential security risks associated with that usage.
B. Secure AI Access Platform:
    1. Provide a secure, managed platform or gateway that allows City staff to access Large Language Models (LLMs) while ensuring enterprise-grade data privacy.
    2. Data Privacy Requirement: The solution must ensure that City data (e.g., Police reports, HR documents) is not used to train public AI models.
C. Policy & Governance Development:
    1. Assist the City in drafting "Acceptable Use Policies" for AI to ensure compliance with Federal and State regulations.
    2. Provide guidance for high-risk departments (e.g., Police Department usage of AI for case reporting).
D. Training & Education:
    1. Provide training resources to educate City employees on the safe and effective use of AI tools to improve productivity without compromising security.

PART 4 - REQUIRED SUBMITTAL FORMAT & PRICING

Proposers must describe their reporting capabilities and provide samples for the following:

A. Executive Dashboards: Real-time views of asset health, ticket status, and security compliance.
B. Asset Management: Automated tracking of hardware lifecycle, warranty status, and software inventory.
C. Strategic Reviews: Process for Strategic reviews to discuss budget and roadmap.
D. AI Governance Reporting: Reports detailing unmanaged AI usage (unauthorized AI tools) detected on the network and user adoption metrics for approved AI platforms.
    1. *Requirement:* Attach sample reports.
E. APPROACH AND METHODOLOGY
   Proposer must respond to the following regarding the entire scope of work:
    1. Support Philosophy: Describe the strategy for balancing proactive security (Part 1) with reactive support (Part 2) and innovation (Part 3).
    2. Support Structure: Describe the team structure and how you ensure familiarity with the City's complex environment (Police, Water, Public Works).
    3. Service Level Objectives (SLOs): Define response targets for Critical (e.g., 30-min), High, and Low priority issues.
    4. Escalation: Explain the path from Tier 1 Help Desk to Tier 3 Engineering and CSM engagement.
    5. Co-Managed Options: Describe how your toolsets allow internal City IT staff to collaborate on tickets and access monitoring tools.
    6. Transition Plan: Describe the onboarding process, specifically how you will handle the secure transfer of CJIS credentials and documentation from the incumbent provider.
F. TOTAL COST SUMMARY
   All submittals shall include a transparent cost breakdown covering Part 1 (Security), Part 2 (Support), and Part 3 (AI).
    1. Pricing Model: Clearly state if pricing is Per User, Per Device, or Fixed Fee.
    2. Note: Proposals that do not meet the compliance requirements of Part 1 (CJIS/AWIA) will be rejected.
    3. Itemized Inclusions/Exclusions: Please confirm inclusion of the following in the monthly fee:
        i. Security: 24/7 SOC/SIEM, EDR, and Vulnerability Scanning.
        ii. Support: Remote Help Desk and Onsite Support.
        iii. Maintenance: Microsoft & 3rd Party Patching Tools.
        iv. Backups: Office 365 (Exchange/OneDrive/SharePoint) Backup Licenses.

v. AI Governance: Secure AI Gateway Platform and unmanaged AI Scanning tools.

4. One-Time Costs:
    i. Onboarding/Transition Fees.
    ii. Initial AI Assessment & Policy Implementation Fees.
5. Professional Services: Hourly rates for projects outside the managed services scope.

RFP ASSUMPTIONS

A. Acceptance Obligation
    1. An accepted proposal does not place the City under any obligation to award any contract based on the lowest price or any other proposal response criteria. The City values "Best Value" over "Lowest Price," specifically regarding Cybersecurity and Compliance capabilities.
B. Project Budget
    1. The City has established a budget for this project. We believe this budget is sufficient for the completion of the project. The budget will not be shared with any proposer.
C. IT Services Acquisition
D. The acceptance of a proposal does not oblige the City to the services of any participating proposer. The City reserves the right to reject all proposals and not decide.
E. Preparation Costs
    1. All costs associated with proposal preparation are the sole responsibility of the proposer.
F. System Requirements Modifications
    1. After receipt of the proposal, and prior to signing the contract, the City reserves the right to modify the requirements by adding or deleting specific services based on the findings of final contract negotiations.
G. Infrastructure Status & Remediation
    1. The City acknowledges that the network currently contains legacy operating systems (e.g., Windows Server 2012, Windows 7) as noted in the Technology Profile. It is assumed that the selected Vendor will prioritize the remediation or replacement of End-of-Life (EOL) assets during the first 12 months of the contract. The proposal should assume the City is willing to budget for necessary hardware/software upgrades to meet security standards.
H. Specialized Vendor Cooperation (SCADA/HVAC)

1. The City utilizes specialized 3rd party vendors for Water/Sewer SCADA (Dorsett Controls) and HVAC (ATC/Yamas). The assumption is that the Managed Services Provider (MSP) will manage the network transport, server hardware, and security for these systems, but will coordinate with the specialized vendors for application-specific support.

I. Mandatory Federal (FBI) and State (Utah BCI) Compliance:
Due to the scope including the Moab Police Department and administrative access to systems connected to the Utah Criminal Justice Information System (UCJIS), the selected Vendor serves as the agency's Information Technology Specialist. The proposal must confirm adherence to both FBI CJIS Security Policy and Utah Bureau of Criminal Identification (BCI) regulations, specifically:
    1. State-Level Background Checks & Rap Back: In addition to national fingerprinting, all Vendor staff with logical or physical access must be fingerprinted and enrolled in the Utah "Rap Back" service (continuous criminal history monitoring) through the Utah BCI, as outlined in UCJIS Policy 6.1.
    2. Non-User Security Agreements: All assigned technicians are classified as "Non-Users" (IT staff with unescorted access) and must sign and submit the official Utah BCI Non-User Security Agreement prior to accessing the network (UCJIS Policy 3.4).
    3. Mandatory Training (Biennial):
        i. Federal: Technicians must hold current CJIS Security & Privacy Training (Level 4 / Privileged Role).
        ii. State: Technicians must complete UCJIS Training and Proficiency Testing initially and every two years thereafter, as required by Utah Administrative Rule R722-900 (UCJIS Policy 3.4).
    4. Local Agency Security Officer (LASO) Designation: The Vendor must designate a specific senior technician to serve as the Local Agency Security Officer (LASO) for the City. This individual will act as the primary liaison with the Utah BCI for technical security compliance and audit preparation.
    5. Misuse & Penalties Acknowledgement: Vendor acknowledges that unauthorized access, use, or dissemination of records is a Class B Misdemeanor under Utah Code Annotated § 53-10-108, punishable by criminal and civil penalties.
    6. Media Destruction Compliance: Vendor must comply with Department of Defense (DoD) 5220.22-M standards for wiping or physically destroying computer hard drives and media when they are no longer used (UCJIS Policy 6.4).

J. Accuracy of Asset Counts

1. Pricing submitted in this proposal is based on the device counts provided in the Technology Profile/Runbook. It is assumed that during the Onboarding Phase, a true-up of assets will occur. If the actual device count varies by more than 10%, the contract price may be adjusted accordingly.

K. Transition Cooperation
   1. It is assumed that the incumbent provider will cooperate in a professional manner to transfer administrative credentials, documentation, and domain access to the selected Vendor upon award of the contract.

AWARD CRITERIA

Evaluation Criteria and Basis of Award (Best Value)

The City intends to award to the most qualified responsible Proposer whose proposal is determined to provide the Best Value to the City, considering the evaluation factors and weights set forth below. Price is not the sole determining factor. The City may select a higher-priced proposal if the City determines that the technical approach, security posture, risk reduction, or overall benefits justify the additional cost.

Proposals will be evaluated using a consensus scoring method. Evaluators may request clarifications, conduct interviews, and/or verify references as part of the evaluation. The City reserves the right to reject any or all proposals, waive informalities, and accept the proposal deemed most advantageous to the City.

Evaluation Factors and Weights

Evaluation Factor	Weight
1. Technical Approach and Security Compliance	25%
2. Innovation and AI	25%
3. Support Experience	20%
4. Experience and Past Performance	10%
5. Qualifications and Certifications	10%
6. Cost	10%
Total	**100%**

A. Technical Approach and Security Compliance (25%)
   The City will evaluate the Proposer's ability to meet the requirements in the Scope of Services and to deliver services in a manner consistent with applicable regulatory and security mandates. Considerations include, but are not limited to:

1. Compliance Alignment: Demonstrated capability to meet the specific mandates applicable to City operations, including CJIS (Police), AWIA (Water/SCADA), and PCI-DSS (payment environments). Proposals should clearly describe how the Proposer will support compliance obligations (e.g., policies, procedures, audit support, documentation, and control mapping where applicable).
2. Security Maturity: The extent to which the Proposer's security program includes advanced security measures (e.g., 24/7 SOC/SIEM monitoring, alert triage/escalation, incident response processes, and EDR) rather than basic antivirus or reactive support.
3. Complexity Management: Demonstrated ability to support complex, hybrid environments, including legacy infrastructure remediation, virtualization (Hyper-V), and Public Safety applications (e.g., Spillman/Fatpot). Proposals should address how the Proposer will manage operational risk, continuity, and security in these environments.

B. Innovation and AI (25%)
The City will evaluate the Proposer's ability to support modernization and strategic planning, including innovation, governance, and executive-level guidance. Considerations include, but are not limited to:
1. AI Governance: Capability to provide tools and strategy for Artificial Intelligence Governance, including the ability to detect and manage Shadow AI usage and to provide a secure, private AI gateway or comparable controls for City staff to use AI in a managed manner.
2. Strategic Planning (vCIO): Quality and maturity of the proposed vCIO process, including the frequency and structure of strategic reviews (quarterly and/or bi-annual), technology roadmaps, budget planning support, lifecycle planning, and executive stakeholder engagement.
3. Reporting and Visibility: Availability of executive reporting and for asset health, security posture, and ticket transparency, including the Proposer's approach to KPIs and service reporting.

C. Support Experience (20%)
The City will evaluate the Proposer's service delivery model and the anticipated experience for City staff and departments. Considerations include, but are not limited to:
1. Team Structure and Consistency: Support model (e.g., pod-based model vs. general queue), assigned roles, escalation paths, after-hours coverage, and the ability to provide consistent, familiar support personnel.

2. Service Levels: Commitment to service level objectives and responsiveness, including the Proposer's ability to meet 30-minute response times for critical outages and the clarity of severity definitions, response/restore targets, and service reporting.
3. Onboarding and Transition: Clarity and completeness of the onboarding and transition plan, including secure transfer of credentials, documentation, configurations, asset inventories, and operational knowledge from the incumbent provider.

D. Experience and Past Performance (10%)
The City will evaluate the Proposer's relevant experience and demonstrated success in similar environments. Considerations include, but are not limited to:
1. Municipal Experience: Track record serving local government clients of similar size and scope, including experience in public safety and/or utility/SCADA environments where applicable.
2. References: Quality and relevance of references, with preference for references from other municipalities, public safety agencies, or similarly regulated environments. The City may contact references and consider the results as part of the evaluation.

E. Cost (10%)
The City will evaluate proposed pricing for clarity, transparency, and overall value. Considerations include, but are not limited to:
Pricing Model and Transparency: Clarity of fee structure (e.g., fixed fee vs. hourly), identification of what is included/excluded, rate schedules, assumptions, and optional services. Total Cost of Ownership (TCO): Total anticipated cost over the contract term, including recurring fees, tool/licensing costs, onboarding/transition costs, and any anticipated pass-through expenses. The City will consider whether costs are predictable and aligned with the proposed technical and security benefits.

F. Preferred, Licenses, Certifications, and Experience (10%):
Proposers should demonstrate staff certifications relevant to the City's specific environment, including but not limited to:

1. Cybersecurity & Compliance:
    - CISSP (Certified Information Systems Security Professional) – Preferred
    - CISA (Certified Information Systems Auditor) or equivalent experience with CJIS Audits. – Preferred
2. Utah BCI Compliance:
    - Experience preparing agencies for triennial Utah Bureau of Criminal Identification (BCI) technical audits.
3. Infrastructure & Cloud:
    - Microsoft Certified: Azure Administrator Associate
    - Microsoft 365 Certified: Enterprise Administrator Expert
    - Legacy Support: Experience supporting Windows Server 2012/2016/2019 and Microsoft Hyper-V environments.
4. Specialized Municipal Experience:
    - SCADA: Demonstrated experience securing network transport for Water/Wastewater SCADA systems.
    - Public Safety: Experience supporting Police Departments, including Spillman, Fatpot, Evidence Library software, and Absolute NetMotion VPN.

SUBMITTAL PACKAGE

Proposals

The City wants the respondents to present their "best solution" for the needs specified in the RFP. This RFP is intended to provide a baseline of information from which the proposer can evaluate and propose additional and/or alternative services. Proposers should use their knowledge and experience within the IT services and security industry to recommend creative solutions that will meet or exceed the RFP requirements, including offering specific options and ideas to create a reliable, functional, and cost-effective solution.

Submission Format

Proposals shall be submitted as a single PDF file, labeled with the firm's name. Submittals shall be forwarded to the Purchasing Agent via email as indicated, prior to the due date and time indicated on Page 1. The submittal should address all requests within this RFP and specifically document the project using appropriate text, graphs, tables, or information necessary to describe the project.

Page Limit & Formatting

To allow for adequate description of the Security and AI solutions requested, submittals shall not exceed 20 pages (two-sided) of text and images (exclusive of résumés, sample reports, and sample contracts). The minimum font size is 11. The City desires submittals that are clear, concise, and specific to the needs and conditions of this project.

Proposal Organization
The proposal shall be organized using the following format:

A. Executive Summary
   Include a brief summary of your firm's proposal. This section shall succinctly explain the firm's interest in the project and its understanding of the City's specific environment (e.g., Public Safety, Water Infrastructure). It shall also contain the name, contact details, and signature of the person authorized to make formal commitments on behalf of the firm.
B. Proposal Details (The Solution)
   Include a detailed description of your response with regard to satisfying the proposed scope of work. Responses should be organized according to the categories listed in the Scope of Services:
   1. Part 1: Cyber Security & Compliance (Address CJIS, SCADA, and SOC capabilities).
   2. Part 2: IT Support Services (Address Help Desk, Onsite Support, and vCIO).
   3. Part 3: AI Governance & Strategy (Address Unmanaged AI detection and Secure AI platforms).
C. Company Qualifications & Experience
   Provide a brief profile of the proposer, including:
   1. Full legal name, year established, and number of employees.
   2. Municipal Experience: specific experience supporting Local Government, Police Departments (Spillman/CJIS), and Public Works (SCADA).
   3. Partnerships: Outline key technology partnerships relevant to the City's profile (e.g., Microsoft, Dell, SonicWall, Ubiquiti, Synology).
D. References
   All proposers must provide a minimum of three (3) references from previous projects of equivalent size and scope.
   1. *Requirement:* At least one reference must be a Government or Public Safety entity to verify CJIS compliance capabilities.
E. Implementation & Onboarding Plan
   Describe the timeline and methodology for onboarding. Specifically address how you will manage the transfer of documentation, credentials, and knowledge from the incumbent provider.
F. Sample Documentation
   Attach examples of the reports required in the Scope of Services, including:
   1. Monthly Executive Summary (System Health).

2. Asset Lifecycle Report.
3. AI Risk/Usage Report.

G. Total Cost Summary
Provide the cost breakdown as defined in Part 4, clearly distinguishing between One-Time Onboarding fees and Recurring Monthly costs.

H. Contract Documents & Exceptions
Copies of proposed support contracts, Service Level Agreements (SLAs), and any exceptions to the City of Moab Proposal Submittal Requirements.

GENERAL INFORMATION

A. Tax Exemption
The City is exempt from all local, state, and federal taxes.

B. Business Licensing
The Selected Consultant must have or obtain a current City of Moab Business License prior to initiating work on this project.

C. Taxpayer Identification
The Selected Consultant must complete a W-9 form (Taxpayer Identification No.).

D. Non-Disclosure & Data Privacy
The City will require the execution of a Mutual Non-Disclosure Agreement (NDA) with the selected consultant(s). This agreement will specifically address the protection of Personally Identifiable Information (PII), CJIS (Criminal Justice Information Services) data, and the restriction of using City data for public Artificial Intelligence (AI) model training.

E. Right of Refusal
The City reserves the right to reject any and all proposals, to waive any informalities or minor irregularities in proposals, and to accept the proposal deemed, in the opinion of the City of Moab, to be in the best interest of the City.

F. Multiple Awards
The City reserves the right to award these services to multiple vendors with multiple contracts (e.g., separating Physical Cabling from Managed Services) if deemed advantageous.

G. Ethics Disclosure
As per the Municipal Officer's and Employee's Ethics Act, applicable disclosures must be made to the City on behalf of any owner, agent, or employee of the proposing firm.

H. Background Checks (CJIS Compliance)
Due to the Scope of Services including support for the Moab Police Department and access to the CJIS network (Spillman/Fatpot systems), the Selected Consultant must ensure that all staff assigned to this account are capable of passing a fingerprint-based background check in accordance with FBI CJIS Security Policy.

I. Cancellation

The City reserves the right to cancel or modify the terms of this RFP and/or the project at any time and for any reason before contract award and reserves the right to accept or reject any or all proposals submitted pursuant to this RFP for any reason. The City will provide each vendor with written notice of any cancellation and/or modification.

J. Public Records

As a public entity, the City is subject to the Utah Government Records Access Management Act, Chapter 63G-2 of the Utah Code. As such, all documents that potential vendors may submit in response to this RFP may be classified as a public record subject to public disclosure.

K. Certification Compliance

All vendors must comply with all applicable federal, state, and local laws and regulations, including compliance with all applicable certification requirements.

L. Award Subject to Negotiations and Execution of Contract

All awards the City may make under this RFP are subject to the negotiation and execution of a contract between the City and the vendor that is acceptable to both parties.

INSURANCE:

A. The Successful Contractor shall not commence work under this Agreement until it has obtained all insurance required by the contract documents. The Contractor shall not allow any subcontractor to commence work on this project until all similar insurance required of the subcontractor has been obtained.
B. The Successful Contractor shall procure and maintain, at its own cost, the following policy or policies of insurance. The Contractor shall not be relieved of any liability, claims, demands, or other obligations assumed pursuant to the contract documents by reason of its failure to procure or maintain insurance in sufficient amounts, durations, or types.
C. The Successful Contractor shall procure and maintain the minimum insurance coverages listed below. Such coverages shall be procured and maintained with forms and insurers generally carrying an A.M. Best rating of "A-" or better.
    1. Workers' Compensation ($1,000,000):
       Insurance to cover obligations imposed by the Workers' Compensation Act of Utah and any other applicable laws for any employee engaged in the performance of Work under this contract.
    2. Commercial General Liability (CGL):
       With minimum single limits of One Million Dollars ($1,000,000) each occurrence and Two Million Dollars ($2,000,000) aggregate.
        i. The policy shall be applicable to all premises and operations.
        ii. The policy shall include coverage for bodily injury, broad form property damage, personal injury (including coverage for contractual and employee acts), independent contractors, products, and completed operations.
    3. Technology Professional Liability (Errors & Omissions):
       With minimum limits of Four Million Dollars ($4,000,000) per claim and aggregate.
        i. The policy shall specifically cover liabilities arising from the Consultant’s acts, errors, or omissions in rendering computer or information technology services, including but not limited to software failure, security failure, and failure to perform professional services.
    4. Network Security & Privacy Liability (Cyber Insurance):
       With minimum limits of Four Million Dollars ($4,000,000) per claim and aggregate.
        i. This coverage is mandatory due to the scope involving CJIS (Police), PCI (Financial), and SCADA (Infrastructure) data.
        ii. The policy must include coverage for:

1. Network Security Liability: Third-party liability arising from a security breach, unauthorized access, or introduction of a virus/malware.
2. Privacy Liability: Liability for the theft, loss, or unauthorized disclosure of Personally Identifiable Information (PII) or Protected Health Information (PHI).
3. Data Breach Expenses: Costs associated with forensic investigation, notification to affected individuals, and credit monitoring services.
4. Ransomware/Extortion: Coverage for ransom payments and negotiation costs.

5. Third-Party Crime / Employee Dishonesty:
   With minimum limits of Five Hundred Thousand Dollars ($500,000).
6. Coverage to protect the City against loss of money, securities, or property resulting from the dishonest acts of the Contractor's employees while performing services on City premises or accessing City systems.
7. Comprehensive Automobile Liability:
   With minimum combined single limits for bodily injury and property damage of not less than One Million Dollars ($1,000,000) each occurrence and aggregate with respect to each of Contractor's owned, hired, and/or non-owned vehicles assigned to or used in performance of the services.

D. The policies required above (except Workers' Compensation and Professional Liability) shall be endorsed to include The City, its officers, officials, employees, and volunteers as additional insureds. Every policy required above shall be primary insurance, and any insurance carried by the City shall be excess and not contributory insurance to that provided by the Contractor.
E. Certificates of insurance shall be completed by the Contractor's insurance agent as evidence that policies providing the required coverages, conditions, and minimum limits are in full force and effect. Copies shall be forwarded to the City prior to the start of Work. Each certificate shall provide that the coverages afforded under the policies shall not be cancelled, terminated, or materially changed until at least 30 days prior written notice has been given to the City.

Failure on the part of the Contractor to procure or maintain policies providing the required coverages shall constitute a material breach of contract upon which the City may immediately terminate the contract.

The City utilizes the State of Utah Purchasing Portal (Utah Public Procurement Place – Bonfire) for procurement activities. This RFP, including all addenda and official communications, will be posted through the portal. Firms interested in responding must register on the State of Utah Purchasing Portal to receive notifications and submit proposals electronically through the system.