Addendum No. 1

Request for Proposal: Managed Information Technology (IT) Service Provider

Issued: April 15, 2026

Questions and Responses

Request for Proposal No.: 2026-01-IT
RFP Contact: Lindsey Nash
Telephone: 403-946-5565 ext. 231
Email: lindseyn@crossfieldalberta.com

Posted to: Alberta Purchasing Connection at https://purchasing.alberta.ca/
Town of Crossfield website at https://crossfieldalberta.com/p/opportunities

PURPOSE OF ADDENDUM

The purpose of this Addendum is to provide clarification and responses to questions received from prospective Proponents regarding the Request for Proposal. The information contained in this Addendum is intended to assist Proponents in the preparation of their submissions. All other terms, conditions, and requirements of the Request for Proposal remain unchanged.

ACKNOWLEDGEMENT OF ADDENDUM

Proponents are required to acknowledge receipt of this Addendum in their submitted proposals. Failure to acknowledge this Addendum may result in disqualification of the proposal.

By acknowledging this Addendum, proponents confirm that they have reviewed and understood the revisions and updates contained herein and have incorporated these changes into their proposal submissions.

QUESTIONS & RESPONSES

- **NOTE:** Due to the volume of questions received during the RFP process, the Town has reviewed and, where appropriate, consolidated similar or duplicate inquiries into a single, comprehensive question.
  This approach is intended to streamline the addendum, reduce redundancy, and ensure clarity and consistency in the responses provided. All efforts have been made to ensure that the intent and substance of each original question have been fully addressed within the consolidated responses.
  Proponents are advised to review all questions and responses in their entirety, as consolidated answers may address multiple related inquiries.

1. PROCUREMENT & GENERAL QUESTIONS	
Question 1	**Would we need to provide a full COR or would a small business just require seCOR?**
Response	The Town will accept either a valid Certificate of Recognition (COR) or Small Employer Certificate of Recognition (SECOR), as applicable based on the size and structure of the Proponent's organization, issued by a recognized certifying partner.
Question 2	**Are you committed to changing your existing vendor or is the incumbent still in consideration?**
Response	As the current contract is nearing completion, the Town is following its procurement policy by issuing a competitive Request for Proposals (RFP). The incumbent vendor is welcome to participate in the RFP process and will be evaluated alongside all other proponents in a fair and transparent manner, based on the criteria outlined in the RFP.

Question 4	**Has the Town established a budget for this engagement, and if so, is there a general budget range or allocation that can be shared?**
Response	The Town has allocated funding for IT services within its approved annual operating budget. Proponents are expected to provide comprehensive pricing based on the full scope of services outlined in the RFP, including managed services, project-based work, and any optional or value-added services. The Town recognizes that costs may fluctuate over the term of the agreement due to factors such as hardware lifecycle and replacement, software licensing renewals, and evolving operational or service requirements.
Question 5	**Is it acceptable for the successful proponent to engage a subcontractor for the provisioning and support of audio-visual services?**
Response	It is acceptable for the successful Proponent to engage a subcontractor for the provisioning and support of audio-visual (A/V) services, provided that the Proponent retains full responsibility and accountability for all services outlined in the RFP. The Proponent must ensure that any subcontractor engaged possesses the appropriate qualifications and experience, and adheres to all requirements, service levels, and standards identified in the RFP. The Proponent will remain the primary point of contact and is responsible for the effective coordination and oversight of all subcontracted work, including installation, maintenance, troubleshooting, and integration of A/V systems. The Proponent is also responsible for ensuring timely response and resolution of issues—particularly during or prior to Council meetings—maintaining system reliability, ensuring compatibility with Town systems, and providing documentation and user support as required. The Town expects that the use of subcontractors will not negatively impact service quality, communication, or response time.
Question 6	**Do you have flexibility to negotiate on the amount of E&O and cyber liability insurance?**
Response	The Town's current insurance requirements reflect guidance received from our insurance provider and are based on our organizational size and risk exposure. Coverage limits for Errors & Omissions (E&O), cyber liability, and general liability have been established at $5 million. These limits represent the Town's minimum requirement and are not expected to be negotiated.

Question 7	**In addition to the objectives outlined in the RFP, are there particular operational challenges, improvement areas, or risk factors that most strongly influenced the decision to seek a new managed IT services partner?**
Response	The primary driver for issuing this RFP is the Town's standard procurement process and the need to re-tender services at the conclusion of the current contract term. In addition, the Town is seeking to ensure continued alignment with industry best practices and maintain a high level of service delivery. Key areas of focus include improving system reliability, strengthening cybersecurity posture, and enhancing long-term IT planning and sustainability. The Town is also seeking opportunities to improve service consistency, documentation, and overall responsiveness, while ensuring scalability to support future operational needs.

2. CYBERSECURITY & COMPLIANCE	
Question 8	**The RFP states that the Town shall retain ownership and control of all cybersecurity platforms, including training systems. Can the Town clarify:** • **Which cybersecurity tools and platforms are currently in place and owned by the Town versus those expected to be supplied by the Proponent; and** • **Whether Proponents are expected to utilize existing Town-selected solutions or may propose alternative platforms (including MDR/EDR, email security, and security awareness training), and if so, whether they may supply and manage such platforms?**
Response	The Town's requirement to retain ownership and control of all cybersecurity platforms, including training systems, is intended to ensure administrative oversight, transparency, and continuous access to cybersecurity tools and data, as well as alignment with internal requirements such as the Town's Health and Safety Program. The Town is also exploring participation in a cybersecurity program through the Canadian Internet Registration Authority. At present, cybersecurity tools and platforms are supplied and managed by the incumbent service provider and are not owned by the Town. A detailed inventory of current systems will be confirmed and shared with the successful Proponent during implementation. Proponents are not required to utilize existing solutions. They may propose alternative cybersecurity platforms, including MDR/EDR, email security, and security awareness training, and may supply and manage these platforms as part of their service offering. All platforms must be established under the Town's administrative ownership and control. The Town currently utilizes cybersecurity awareness training tools; however, no specific platform is mandated. The provision of a training platform is not included within the base scope of this RFP but may be proposed as a value-added service, with all associated costs clearly identified. The successful Proponent will be expected to ensure continuity of cybersecurity services throughout the contract term and support a seamless transition at contract completion, with no disruption to coverage.

Question 9	**Can the Town clarify its expectations for SOC services, including:** • **Which existing security platforms/products are to be monitored;** • **Whether SOC services must be delivered within Canada or if remote/global SOC delivery is acceptable; and** • **Whether the Town requires a fully managed 24×7 SOC with human-led response, or if 24×7 monitoring with alerting and defined escalation procedures is sufficient?**
Response	A detailed inventory of security platforms and related infrastructure will be made available to the successful Proponent during the transition and onboarding phase. In the interim, Proponents should assume a typical municipal IT environment and outline their approach to monitoring commonly used platforms (e.g., endpoint protection, firewalls, email security, and servers). A comprehensive review and validation of existing security platforms will occur during the transition period. The successful Proponent will be expected to assess the current environment and implement their proposed solution, including the replacement or consolidation of existing tools where appropriate. The Town prefers SOC services to be delivered within Canada; however, Proponents may propose alternate or global delivery models. In such cases, Proponents must clearly identify where monitoring services are performed and demonstrate how personal information will be protected through appropriate administrative, technical, and contractual safeguards. Preference may be given to Canadian-based services where data residency or sovereignty considerations apply. The Town requires 24/7 monitoring and incident response capabilities. A fully managed 24×7 Security Operations Center (SOC) with human-led response is preferred; however, the Town will consider solutions that provide 24/7 monitoring with alerting and defined escalation procedures, provided that timely and effective incident response can be clearly demonstrated. Proponents should clearly describe their SOC approach, including monitoring scope, response capabilities, escalation procedures, and incident triage and resolution processes, in alignment with the service level expectations outlined in the RFP. The successful Proponent will be expected to ensure continuity of cybersecurity services throughout transition, with no disruption to monitoring or incident response coverage.

Question 10	**The RFP references regular internal and external vulnerability assessments and periodic cybersecurity risk assessments. Can the Town clarify:** • **The expected frequency (e.g., monthly, quarterly, annually); and** • **The required depth of these assessments (e.g., automated vulnerability scanning versus manual penetration testing), including reporting expectations?**
Response	As outlined in Section 4.3 of the RFP, the Town requires regular internal and external vulnerability assessments, along with periodic cybersecurity risk assessments. The Town has not prescribed a specific frequency or depth for these assessments. Proponents are expected to propose an approach that aligns with industry best practices and the size and complexity of the Town's environment. This should include clearly defined frequency (e.g., monthly, quarterly, annually), methodology (e.g., automated vulnerability scanning and risk assessments), and reporting on identified risks and recommended remediation actions. Where more advanced assessments, such as manual penetration testing, are proposed, these should be clearly identified and priced separately as optional or project-based services.
Question 11	**Can the Town clarify its data residency requirements, including:** • **Whether specific systems or datasets must reside exclusively within Canada;** • **Whether disclosure or exceptions are acceptable where Canadian residency is not feasible; and** • **Whether Microsoft-controlled data residency mechanisms are considered acceptable for compliance purposes?**
Response	The Town has not identified specific systems or datasets that must reside exclusively within Canada. However, as outlined in the RFP, Proponents are expected to ensure that municipal data is stored within Canada where feasible, particularly where sensitive or personal information is involved. Where Canadian data residency is not feasible, the Town will accept solutions that involve data storage outside of Canada, provided that Proponents clearly disclose these instances and demonstrate how personal information will be protected in compliance with applicable Canadian privacy legislation. This must include appropriate administrative, technical, and contractual safeguards. Microsoft-controlled data residency mechanisms are considered acceptable for compliance purposes, provided that Proponents clearly demonstrate how these controls align with applicable Canadian privacy legislation and ensure appropriate protection of personal information. The Town may give preference to solutions that maintain data residency within Canada, where feasible.

Question 12	**Is the Town willing to accept risk-based SLA adjustments for large-scale cyber incidents**
Response	The Town recognizes that large-scale cyber incidents may impact standard SLA performance. Reasonable, risk-based adjustments may be considered during such events, provided there is clear communication, documented justification, and continued prioritization of critical services and incident containment.

3. INFRASTRUCTURE & TECHNICAL ENVIRONMENT	
Question 13	**Can the Town clarify its current backup and disaster recovery environment, including:** • **Whether the backup system is owned by the Town or provided by the incumbent/vendor;** • **The current backup software vendor and offsite storage solution in use;** • **Whether offsite disaster recovery infrastructure is Town-owned or provided by a third party, and whether Proponents are expected to quote for replacement or only management; and** • **The role and configuration of NAS devices within the environment, including whether they are used for enterprise storage, backups, or both.**
Response	The Town's backup and disaster recovery environment includes both Town-owned infrastructure and services provided by the incumbent Managed IT Service Provider. The Town owns its Network Attached Storage (NAS) devices, which are used for local backups and operational storage, including body-worn camera video data. Replacement of this infrastructure is not specifically anticipated; however, Proponents may recommend improvements with associated costs clearly identified. The Town currently utilizes Veeam Backup & Replication, with licensing, offsite storage, and disaster recovery services provided and managed by the incumbent and not owned by the Town. Proponents are expected to include backup software licensing, offsite storage, and disaster recovery services as part of their proposed solution, whether through continuation or replacement. All associated costs should be clearly outlined.
Question 14	**Are all server VMs Windows-based or are there other operating systems utilized?**
Response	The Town's server environment is primarily Windows-based; however, it also includes a limited number of Linux-based virtual machines. The majority of virtual servers run Microsoft Windows Server (including Windows Server 2022 and Windows Server 2012 R2). Linux-based virtual machines are utilized for specific functions, including network management and VPN services. The Town also operates physical servers running Microsoft Windows Server 2022, including Hyper-V hosts. In addition, the current telephone system is supported by a standalone 3CX server hosted on hardware that is no longer under warranty**.**

Question 15	**Can the Town provide a detailed network and infrastructure overview, including (or via a network diagram if available):** • **Number and make/model of firewalls, routers, switches, and access points;** • **Number of ISPs and service providers at each location;** • **Technologies and vendors supporting interconnectivity between locations; and** • **A summary of all core infrastructure components (servers, networking equipment, etc.)**.
Response	The Town's network and infrastructure environment consists of a combination of centralized and distributed components supporting connectivity across multiple municipal facilities. Interconnectivity between locations is primarily achieved through radio links utilizing Ubiquiti (UBNT) microwave technology in a point-to-multipoint configuration. The Fire Hall radio tower serves as the central hub, providing connectivity to remote buildings. The Town currently maintains two separate fiber-based internet service connections, located at the Town Hall and Fire Hall facilities. From a network security perspective, the Town utilizes two Ubiquiti UniFi Security Gateways. Aside from these gateway devices, the network environment is relatively streamlined, with no additional standalone firewall infrastructure currently in place. A detailed inventory of network hardware (including switches, access points, and other infrastructure components) will be made available to the successful Proponent during the transition and onboarding phase. Proponents may identify and recommend improvements or upgrades as part of their submission, with associated costs clearly outlined if applicable.
Question 16	**Can the Town provide details on any additional technologies expected to be managed, including:** • **Camera systems (number of cameras, type such as CCTV or cloud-based, and management expectations); and** • **Audio/visual systems (number and types of rooms such as council chambers, boardrooms, etc., and associated support requirements).**
Response	The Town's camera systems consist of approximately 25 CCTV cameras across four (4) Town facilities. These systems are owned and operated by the Town. The successful Proponent will be responsible for ensuring that the network connectivity supporting these systems remains operational; however, full management of the CCTV system itself is not within the core scope of services. In addition, there is a single camera located in Council Chambers used for live streaming of meetings. This system may require limited support from the Proponent in relation to functionality and integration with broadcasting or streaming platforms. The Town has four (4) rooms equipped with audio/visual (AV) technology, including the Council Chambers, Administration Boardroom, Fire Department Boardroom, and Operations Boardroom. The successful Proponent will be responsible for supporting these AV systems, including basic troubleshooting, maintenance, and ensuring functionality for meetings and operational use.

Question 17	**Can the Town clarify its current security environment, including:** • **Whether additional tools beyond Microsoft 365 native security (e.g., email security, content/internet filtering) are in place and expected to be managed; and** • **Whether Proponents are expected to provide any additional security or monitoring technologies (beyond MDR), or if all required tools are currently in place and only require management.**
Response	The Town of Crossfield utilizes a combination of Microsoft 365 native security features and additional security measures within its IT environment. Proponents should assume that security controls extend beyond Microsoft 365 and may include tools such as email security, endpoint protection, and network/content filtering. The successful Proponent will be expected to manage and support these security technologies as part of the overall service delivery. At the same time, the Town's security environment may evolve over the course of the contract. Proponents are therefore encouraged to outline their approach to assessing the existing environment and recommending enhancements where appropriate. Proponents may propose additional security and monitoring technologies (beyond MDR) where they believe it will strengthen the Town's cybersecurity posture. Any proposed solutions should clearly identify the value provided, integration with existing systems, and ongoing management requirements. The Town is open to considering both the continued use of existing tools and the introduction of new solutions, where justified. The Town of Crossfield's fire alarm systems are monitored and managed by a third-party provider and are not included within the scope of this RFP. The successful Proponent will only be responsible for ensuring that network connectivity supporting these systems remains operational.
Question 18	**Disaster Recovery Testing: Does the Town require annual disaster recovery exercises, and are there specific RTO/RPO targets for critical systems?**
Response	The Town requires the successful Proponent to conduct annual disaster recovery (DR) exercises to validate the effectiveness of backup and recovery processes, confirm system recoverability, and ensure overall organizational readiness in the event of a disruption. At this time, the Town has not established formalized Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all systems. The successful Proponent will be expected to work collaboratively with the Town during the onboarding and transition phase to: • Identify and classify critical systems and services; • Recommend appropriate RTO and RPO targets based on operational requirements and risk tolerance; and • Implement and maintain disaster recovery strategies aligned with those targets. Disaster recovery testing should include documented results, identification of gaps or risks, and recommendations for continuous improvement. The frequency and scope of testing may be expanded where warranted, particularly for systems identified as critical to municipal operations.

4. SUPPORT MODEL, SLA & OPERATIONS	
Question 19	**Can the Town clarify its expectations regarding SLA structure and performance management, including:** • **The weighting of response and resolution time requirements, and whether these are negotiable or pass/fail criteria;** • **The point at which response and resolution times are measured (e.g., ticket submission, acknowledgment, or assignment);** • **Whether SLA performance will be evaluated on an incident-by-incident basis or through aggregated reporting (e.g., monthly or quarterly); and** • **Any high-level principles regarding the application of service credits or corrective actions for repeated SLA non-compliance.**
Response	Response and resolution time requirements are evaluated as part of the *Approach, Timelines and Communication* criterion, which carries a weighting of 20% of the overall score. These are not strict pass/fail requirements; however, they are a significant component of the evaluation. Proponents are expected to demonstrate their ability to meet or exceed desired service levels, including response times, resolution targets, escalation procedures, and service coverage. The Town is open to refining these expectations with the preferred Proponent during contract negotiations. As outlined in the RFP, response time is measured from the time an incident is reported through an accepted channel (e.g., helpdesk ticket, email, phone, or monitoring alert) to the time the Proponent acknowledges and begins working on the issue. Resolution time is measured from the time the incident is reported to the time service is restored or a reasonable workaround is implemented, in accordance with defined Service Level Agreements (SLAs). SLA performance will be evaluated primarily through aggregated monthly reporting, including metrics such as response times, resolution times, ticket volumes, and recurring issues. Individual incidents may be reviewed on an exception basis, particularly where service levels are not met or where incidents significantly impact operations. The Town's approach to SLA management is focused on continuous improvement and accountability. In cases of repeated or systemic non-compliance, the Proponent may be required to implement corrective action plans. Service credits or fee adjustments may be considered where performance issues persist; however, specific terms and thresholds will be defined during contract negotiations.

Question 20	**Can the Town clarify its expectations for A/V support, including:** • **The level and scope of A/V services required;** • **How A/V-related incidents are prioritized, including whether Council Chambers issues during active meetings are considered Priority 1 incidents; and** • **Whether there are specific systems, departments, or services considered especially time-sensitive or operationally critical that would require elevated prioritization.**
Response	The Town's A/V support requirements are primarily focused on Council Chambers, including microphones, cameras, and live streaming. The Proponent will be expected to provide troubleshooting and support as needed, including timely remote guidance during meetings to minimize disruption. A/V-related incidents are generally classified as medium priority (Priority 3), with a response time of within one (1) business day. Issues during active meetings are not typically considered Priority 1; however, where functionality is significantly impacted, the Proponent is expected to make reasonable efforts to provide immediate support. In addition to A/V systems, the Town considers certain services to be operationally critical, including SCADA, VoIP, and core network infrastructure. Incidents impacting these systems may be treated with elevated priority due to their importance to operations and service continuity.
Question 21	**How frequently are after-hours incidents currently experienced?**
Response	After-hours incidents are rare, typically occurring only a few times per year and primarily related to individual employee issues or specific system incidents.
Question 22	**Does the Town envision a fully outsourced MSP model, or will there be shared responsibility with internal IT resources?**
Response	The Town envisions this as a fully outsourced Managed Service Provider (MSP) model. The Town does not maintain in-house IT resources. Internal involvement is limited to minimal administrative coordination, such as facilitating new technology purchases, supporting major issue escalation, and providing general liaison support between the MSP and Town departments.

5. SERVICE DELIVERY MODEL & ONSITE SUPPORT	
Question 23	**The RFP references quarterly on-site support for non-emergent services. Can the Town clarify its expectations regarding service delivery, including:** • **Whether the Town is open to a hybrid support model (combining remote and scheduled on-site support, such as monthly visits);** • **The overall expectation for on-site versus remote support delivery;** • **Expectations for technical support during Council meetings or special sessions (e.g., on-site, remote, or hybrid); and** • **Any after-hours or event-based support requirements for scheduled meetings, including advance readiness checks or standby support.**
Response	The Town is open to a hybrid support model that includes a combination of remote support and scheduled onsite services. While the RFP identifies quarterly onsite visits, Proponents may propose alternative approaches (e.g., monthly onsite hours), provided that pricing reflects the level and frequency of onsite service. The intent of scheduled onsite visits is to reduce ad hoc, non-emergency callouts by addressing lower-priority items that benefit from in-person support, such as device installations, ongoing issue resolution, and small project-based work. Overall, the Town anticipates a primarily remote support model supplemented by periodic onsite services. For Council meetings and special sessions, the Town expects a hybrid approach. Administration will typically be onsite to manage operations, while the Proponent is expected to provide remote IT-level support as needed. Onsite MSP presence is not typically required but may be requested in advance for specific situations. After-hours or event-based support requirements are expected to be limited. Support for scheduled meetings is generally provided on an as-needed basis, primarily to ensure continuity of service where issues significantly impact meeting functionality or core systems. The Town does not require dedicated standby resources; however, advance readiness checks and remote support should be available where appropriate.
Question 24	**Council Chamber A/V Support: Does the Town expect the MSP to provide full in-room, operational A/V support during meetings, or IT-level support with coordination of an A/V vendor?**
Response	The Town does not expect the MSP to provide full in-room, operational audio/visual (A/V) support during Council meetings. The expectation is for IT-level support, including troubleshooting and coordination with third-party A/V vendors where required. A/V-related issues are generally classified as medium priority (Priority 3), with an expected response time of within one (1) business day. Issues occurring during live meetings are not typically considered Priority 1; however, where functionality is significantly impacted, the Proponent is expected to make reasonable efforts to provide timely guidance or support to assist Administration in resolving issues in real time.

Question 25	**Is the MSP expected to provide operational coordination only, or also assist with contract renewals and SLA reviews?**
Response	The MSP is expected to provide both day-to-day operational coordination and support for vendor contract lifecycle activities. This includes coordinating and escalating vendor-related issues, troubleshooting, and ongoing communication with third-party providers, as well as assisting the Town with contract renewals, service reviews, and providing recommendations on vendor performance and SLA alignment. Final decision-making authority for vendor selection, contract approvals, and renewals will remain with the Town.

6. USERS, DEVICES & SUPPORT VOLUME	
Question 26	**Can the Town provide a detailed overview of the IT environment, including:** • **Total number of employees and users (full-time equivalent), including distinctions between office staff requiring full IT management and other users (e.g., fire fighters, external or limited-access accounts);** • **The number and types of supported assets (e.g., workstations, network endpoints, servers, backup environment); and** • **How endpoints are deployed (e.g., office-based, remote, or hybrid), including whether shared or kiosk-style workstations are utilized.**
Response	The Town currently supports approximately 40 full-time and part-time staff (FTEs), along with 7 Councillors, all of whom require full IT management and primarily utilize individual workstations. In addition, the Town has approximately 30 Fire Fighters who require limited IT support, primarily related to email access and basic system use. A small number of additional user accounts are maintained for external vendors or service providers and are managed on an as-needed basis. A detailed inventory of supported assets including the number and types of workstations, network devices, servers, and backup systems will be provided to the successful Proponent during the transition and onboarding phase due to security and privacy considerations. The Town's current backup environment is approximately 7 TB in size. Endpoints are deployed in a hybrid model. The majority of users operate from office-based workstations, with some staff enabled for remote work on assigned devices. The Town also utilizes a limited number of shared or kiosk-style workstations, including a front counter computer used for payment processing, as well as shared terminals at the Arena and Fire Hall.

Question 27	**Can the Town provide high-level information on average monthly helpdesk ticket volumes over the past 12 months, including any observable trends and, if available, a breakdown by incident priority level (e.g., P1–P4).**
Response	The Town's average helpdesk volume over the past 12 months is approximately 38 tickets per month. Ticket volumes have remained relatively consistent, with no significant seasonal or operational trends observed. Based on general operational experience, the majority of tickets are classified as medium to low priority (Priority 3–4) and are typically related to individual user support. Common requests include login credential support, printer issues, device troubleshooting, and email-related concerns. High-priority incidents (Priority 1–2) are infrequent. The Town expects Proponents to propose a support model that effectively manages a predominantly user-focused ticket environment, while also supporting proactive maintenance and monitoring activities.
Question 28	**To support capacity planning, can the Town provide an approximate indication of how frequently after-hours or emergency IT incidents have occurred over the past two years?**
Response	After-hours or emergency IT incidents have been infrequent over the past two years. On average, incidents have occurred less than once every two months. The Town expects that this low frequency will continue and that after-hours support will primarily be required for occasional, high-priority issues impacting core systems or municipal operations.

7. SCADA & SPECIALIZED SYSTEM	
Question 29	**Can the Town clarify expectations for SCADA systems, including:** • **The required level of management and support; and** • **Whether centralized logging is currently in place and expected to be maintained or managed as part of the services.**
Response	The Town's SCADA system is currently supported through a combination of service providers. Infrastructure-level monitoring and management of the underlying server environment is handled by the Town's IT provider, while SCADA-specific support (including graphics changes, PLC and RTU modifications, and management of the OPC DA server and clients) is managed by a specialized SCADA vendor. The Town expects this general support model to continue, with the successful Proponent responsible for maintaining the supporting IT infrastructure and coordinating with the SCADA vendor as required. Full SCADA system management is not within the core scope of services. With respect to logging, SCADA system logs are currently collected and stored locally within the SCADA platform. The Town additional server or centralized logging is in place through its current IT provider.

	Proponents may propose enhancements to logging, monitoring, or centralized log management as part of their solution.
Question 30	**What is the architecture of the network?**
Response	The Town's network environment includes a combination of segmented corporate and operational networks. The corporate network supports general business operations, while the water and SCADA control systems operate within a segregated environment behind a firewall. The control network is understood to utilize a relatively flat architecture within its secured boundary, with remote sites (e.g., lagoon facilities) connected via point-to-point wireless links. Network segmentation is in place through the use of VLANs to separate control systems from user workstations and other municipal systems.

8. PRICING & CONTRACT STRUCTURE	
Question 31	**Does the Town have a preferred pricing structure for managed services (e.g., per-user, per-device, hybrid, or fixed monthly), or will all compliant pricing models be evaluated equally?**
Response	The Town is open to evaluating various pricing structures (e.g., per-user, per-device, hybrid, or fixed monthly); however, the Town has a preference for a per-user pricing model that provides a comprehensive, predictable monthly cost. This model should include the full scope of services outlined in Section 4 of the RFP, as well as support for all hardware, software, and systems identified in Schedule B. Proponents may propose alternative pricing structures; however, all submissions should clearly define what is included within the base fee and identify any out-of-scope or additional services as separate, optional costs.

9. ADDITIONAL TECHNICAL & OPERATIONAL QUESTIONS	
Question 32	**Can the Town clarify whether it currently utilizes, or expects Proponents to provide and/or manage, the following platforms:** • **End-user training/learning management systems (e.g., Microsoft 365/Co-Pilot training, excluding cybersecurity awareness training); and** • **Enterprise password management solutions for staff?**
Response	The Town does not currently utilize an end-user training or learning management platform for Microsoft 365 applications, Co-Pilot, or other software applications, aside from cybersecurity awareness training tools. The Town also does not currently utilize an enterprise password management platform across the organization. The supply and management of these platforms are not included within the base scope of this RFP; however, the Town would welcome recommendations from Proponents as potential value-added services. Any proposed solutions should be clearly identified and priced separately as optional or out-of-scope services.
Question 33	**Does the Town of Crossfield employ any microwave or other types of wireless RF links to connect their buildings? If so, is the management of this equipment to be included in the RFP? Does that include such things as equipment replacement inclusive of tower climbing technicians to maintain this equipment?**
Response	The Town utilizes point-to-point wireless (RF) connections from the Fire Hall to eight (8) Town buildings/facilities. Management of this equipment is included within the scope of the RFP, and the Proponent will be responsible for monitoring, maintenance, and troubleshooting. Equipment replacement, including any specialized services such as tower climbing technicians, may be coordinated by the Proponent and contracted as required.
Question 34	**Section 4.9 references the ability to provide prompt response and resolution during or immediately before Council meetings. Can the Town please clarify whether support for Council Chambers technology during scheduled Council meetings occurring outside standard support hours (Monday–Friday, 8:00 a.m. to 8:00 p.m. MST) is expected to be included within the base managed services fee, or whether such after-hours support may be addressed through separate pricing or on-call arrangements?**
Response	The Town expects the Proponent to be available to provide support for Council Chambers technology during scheduled Council meetings, including those occurring outside standard support hours, where required to ensure meeting continuity. Proponents may include this support within their base managed services fee or propose it as a separate or on-call service; however, the approach and associated costs must be clearly defined within the proposal.

Question 35	**Section 4.10 notes that routine municipal IT support is included within the base scope, while additional or optional services are to be clearly defined and priced separately. Can the Town provide clarification on how it distinguishes between managed services and project-based work, particularly for activities such as Council Chambers technology upgrades, major configuration changes, or technology refresh initiatives?**
Response	The Town considers managed services to include day-to-day IT operations, support, maintenance, monitoring, and incident response necessary to maintain the stability and performance of the existing environment. This includes routine support for Council Chambers technology. Project-based work is generally defined as non-routine activities that involve significant changes, upgrades, or enhancements to the Town's IT environment. This includes, but is not limited to, Council Chambers technology upgrades, major configuration changes, infrastructure replacements, and technology refresh initiatives. Project-based work is not included within the base managed services scope and is expected to be scoped, quoted, and approved by the Town prior to proceeding.
Question 36	**With reference to the Priority Level definitions in Section 4.1, can the Town clarify which systems are considered "critical systems" for the purposes of Priority 1 incident classification? Specifically, should Council Chambers audio-visual systems be considered critical systems, or is Priority 1 intended to apply primarily to core municipal operations such as network infrastructure, servers, cybersecurity, emergency services, financial systems, and line-of-business applications?**
Response	Priority 1 is intended to apply primarily to core municipal operations, including network infrastructure, servers, cybersecurity systems, emergency services, financial systems, and line-of-business applications. Council Chambers audio/visual (AV) systems are not typically classified as critical systems for the purposes of Priority 1 incident classification. During meetings, Administration will make reasonable efforts to address and correct AV issues in real time where possible, while minimizing disruption to proceedings. As such, AV-related issues are generally classified as medium priority (Priority 3), with an expected response time of within one (1) business day. However, the Proponent should be available to provide guidance or support during meetings if required, particularly where issues significantly impact meeting functionality.

Question 37	**Appendix B outlines that the Town currently has 9 servers/endpoints with licensing for backup and replication, along with local NAS and offsite storage. Could you please specify which BCDR vendor and software you are currently using?**
Response	The Town currently utilizes Veeam Backup & Replication as its primary backup and disaster recovery (BCDR) solution, supporting its server environment along with local NAS and offsite storage. The successful Proponent will be expected to assess the existing backup and replication environment during the transition phase and confirm its continued suitability. Proponents may recommend enhancements or alternative solutions where they provide clear operational or security benefits, while ensuring continuity of backup and recovery capabilities.

10. STRATEGY, GROWTH & FUTURE STATE	
Question 38	**Can the Town provide expected growth projections over the contract term (e.g., users, devices, facilities, and systems), and confirm whether proponents should incorporate any specific assumptions regarding this growth into their pricing models?**
Response	The Town anticipates modest growth over the contract term, with approximately 1–2 additional users per year. Device growth is expected to align with user growth, with incremental additions of end-user devices as required. The Town does not anticipate significant expansion in the number of facilities or core systems during the contract term. Proponents should consider this level of incremental growth when developing their pricing models. The Town expects that proposed pricing structures can accommodate modest fluctuations in users and devices, while remaining scalable to support future operational needs.
Question 39	**Are project-based services expected to be occasional (exception-based), or a regular component of the engagement?**
Response	Project-based services are expected to be occasional and exception-based rather than a regular component of the engagement. The Town anticipates that the majority of services will be delivered under the core managed services scope, including day-to-day support, maintenance, and vendor coordination. Project services may be required periodically for initiatives such as system upgrades, infrastructure improvements, or new technology implementations, and should be clearly identified and priced separately as outlined in the RFP.

Question 40	**What is the Town's position towards long-term strategies involving cloud server hosting vs. having continued local server hardware to host your servers?**
Response	The Town of Crossfield operates a hybrid IT environment that includes both on-premise (local server hardware) and cloud-based solutions. The Town supports a balanced, strategic approach to infrastructure planning and will continue to evaluate opportunities to leverage cloud hosting where it provides clear advantages, such as scalability, enhanced disaster recovery, cost predictability, and reduced reliance on physical infrastructure. At the same time, the Town recognizes that certain systems, data, or operational requirements may necessitate the continued use of local server hardware. Considerations such as data sovereignty, system performance, integration with existing infrastructure, and risk management will inform these decisions. The Town is seeking a Proponent that can support and manage a hybrid environment, provide strategic guidance on the appropriate balance between cloud and on-premise solutions, and recommend cloud migration opportunities where beneficial, including associated risks, costs, and implementation strategies.
Question 41	**During the anticipated contract term, are there any known or contemplated upgrades, modernization initiatives, or functional enhancements planned for Council Chambers audio-visual or meeting technology?**
Response	At this time, the Town does not have any known or planned upgrades, modernization initiatives, or functional enhancements for Council Chambers audio-visual or meeting technology. The Town may consider future improvements based on operational needs, technology lifecycle, or recommendations provided by the successful Proponent.
Question 42	**How would the Town describe a successful first year of service with the selected proponent, from both an operational and strategic perspective?**
Response	A successful first year of service with the selected Proponent would demonstrate both strong operational performance and meaningful strategic progress. From an operational perspective, success would include consistent, reliable service delivery, clear and ongoing communication, and a comprehensive review of the Town's IT environment. This would include the development and validation of accurate, up-to-date documentation, such as asset inventories, lifecycle planning (including replacement timelines), and overall system architecture. From a strategic perspective, the Town expects the Proponent to provide guidance and recommendations that support continuous improvement, including enhancing service delivery to residents, improving internal processes, strengthening cybersecurity posture, and optimizing document and information management.

11. TRANSITION & DOCUMENTATION	
Question 43	**Does the Town currently have an incumbent Managed IT Service Provider (MSP)? If so, please identify the provider and clarify the Town's expectations regarding transition and onboarding, including:** • **Whether the incumbent will be required to cooperate in transition activities (e.g., documentation transfer, credential handover, and system knowledge sharing), and whether such cooperation will be contractually enforced;** • **Whether the Town will assist in facilitating access should any challenges arise during the transition; and** • **Whether there are any preferred transition timelines, operational sensitivities, or blackout periods that proponents should consider when planning onboarding activities.**
Response	Yes, the Town currently utilizes an external Managed IT Service Provider; however, the name of the incumbent will not be disclosed as part of this RFP process. The Town expects full cooperation from the incumbent provider during any transition activities, including but not limited to documentation transfer, credential handover, and system knowledge sharing. These requirements will be contractually enforced to ensure continuity of service and minimize operational risk. The Town will also support and facilitate the transition process, including assisting with access or coordination should any challenges arise. The current contract is set to expire on May 31. Proponents should anticipate transition activities commencing in the last week of May and continuing into early June. The Town anticipates a transition period of approximately 30–60 days, during which overlap between providers may occur to maintain uninterrupted service. Proponents should be aware of key operational sensitivities when planning onboarding activities. In particular, the issuance of annual tax notices in early May represents a critical operational period, and the Town prefers to avoid any major system changes or disruptions during this time. Proponents are expected to propose a transition approach that minimizes risk and ensures continuity of services during such periods. Relevant information regarding the Town's IT environment, systems, and service delivery will be made available to the successful Proponent during the transition and onboarding phase to support a smooth and informed service commencement. Following award, the Town will coordinate a formal transition meeting to establish detailed timelines, responsibilities, and key milestones. If the incumbent provider is reselected, the Town will still require a structured onboarding or "re-onboarding" process to ensure alignment with current expectations, updated documentation, and service delivery standards

Question 44	**Can the Town provide a high-level view of the current completeness and accuracy of IT documentation (e.g., network diagrams, asset inventories, SOPs, access records), and clarify expectations for documentation deliverables at key milestones (e.g., Day 1 versus within the first 90 days)?**
Response	The Town's existing IT documentation is available but varies in completeness and level of detail across different areas. While certain elements, such as asset inventories and system configurations, are maintained, other documentation (e.g., network diagrams, standard operating procedures, and access records) may require validation, updates, or further development. At contract commencement (Day 1), the Proponent is expected to have sufficient baseline understanding and access to critical systems to support ongoing operations and service delivery. During the onboarding and transition period (first 90 days), the Proponent will be expected to complete a full environmental assessment, validate existing documentation, and develop comprehensive, accurate, and up-to-date documentation in accordance with the RFP requirements. Documentation should be substantially complete, validated, and accessible to the Town by the end of this period, with ongoing updates maintained throughout the term of the agreement.
Question 45	**To support transition planning, can the Town provide a consolidated overview of the core cybersecurity and resilience platforms currently in use (e.g., EDR/MDR, email protection, backup/recovery, security awareness training), beyond the licensing counts listed?**
Response	At this time, the Town has not provided a consolidated or detailed inventory of the specific cybersecurity and resilience platforms currently in use beyond the information already included in the RFP (e.g., licensing counts). A comprehensive overview of the Town's cybersecurity environment including core platforms such as endpoint detection and response (EDR/MDR), email security, backup and recovery solutions, and security awareness training will be made available to the successful Proponent during the transition and onboarding phase. This approach is intended to ensure that the selected Proponent receives accurate, up-to-date, and validated information directly from the current operating environment, supporting an effective transition and informed service delivery. Proponents should, in the interim, assume a typical municipal IT environment and outline their approach to implementing, managing, and optimizing industry-standard cybersecurity and resilience platforms as part of their proposed solution.