Request for Proposals (RFP) 2026-01

Village of Keremeos Complete Information Technology (IT) Services

Managed IT Services / Service Desk / Cybersecurity / Infrastructure / Microsoft 365 / Backup/DR

RFP Issued	July 6, 2026
Questions Deadline	July 27, 2026
Closing Date & Time	Aug 3, 2026
Anticipated Shortlist/Interviews	Aug 17, 2026
Anticipated Award	Aug 31, 2026
Anticipated Service Commencement	The anticipated service commencement date is **October 1st,, 2026** with proponents expected to support transition activities prior to full service commencement.

Procurement Contact: Don Bishop, Village of Keremeos, Box 160, 702-4th Street, Keremeos, BC V0X 1N0, 250-499-2711, operationsmanager@keremeos.ca

Notice: Proponents must direct all communications regarding this RFP to the Procurement Contact only. The Village may issue written addenda; it is the Proponent's responsibility to obtain all addenda and acknowledge them in its submission.

1. Invitation to Proponents

The Village of Keremeos (the Village) invites qualified firms (the Proponent) to submit proposals for complete outsourced IT services on a managed services basis. The successful Proponent will deliver day-to-day support, proactive maintenance, cybersecurity, Microsoft 365 administration, backup and disaster recovery management, vendor coordination, and strategic planning support for the Village's municipal IT environment.

2. Background and Objectives

The Village operates municipal services from multiple locations (e.g., Village Hall, Public Works, and Wastewater Treatment, Victory Hall). The environment includes approximately **14+/- active users**, a mix of desktops/laptops, printers, copiers/MFDs, cell phones/mobile

devices, network equipment (switching and wireless), and security infrastructure including firewalls and business continuity systems.

Definition of IT-related equipment: For the purposes of this RFP, "IT-related equipment" includes desktops, laptops, servers, printers, copiers/MFDs, cell phones/mobile devices, monitors, peripherals, network devices, wireless equipment, telephony-related hardware, and other technology assets used to support Village operations.

Key objectives of this RFP include:

- Provide reliable, responsive end-user support with clear service levels and escalation.
- Improve security posture through layered controls, monitoring, and user awareness training.
- Maintain and document the IT environment (asset inventory, credentials handling, configurations).
- Deliver predictable monthly operating costs, with transparent project and hardware procurement practices.
- Support lifecycle replacement planning aligned to the Village's multi-year IT budgeting.
- Ensure compliance with applicable privacy and records requirements, including BC's Freedom of Information and Protection of Privacy Act (FIPPA).

3. Current Environment (High-Level) and Assumptions

The following information is provided to help Proponents size and price services. Proponents are responsible for validating details during due diligence.

- **Users:** Approximately 14+/-.
- **Endpoints:** Mix of desktops and laptops plus monitors and peripherals.
- **Servers:** At least one on-premises server supporting municipal operations; warranty and lifecycle management required.
- **Network/Security:** Multi-site connectivity with managed firewalls and wireless access points.
- **Microsoft 365:** Tenant administration, identity, email, and collaboration services.
- **Business continuity:** Backup and disaster recovery (BDR) capability is in place; ongoing monitoring, testing, and improvement required.
- **Printers, copiers/MFDs, cell phones/mobile devices, and line-of-business systems:** Various municipal applications and devices requiring vendor coordination, administration, lifecycle tracking, and support.

Assumptions: (a) The successful Proponent will be the primary IT service provider and will coordinate with third-party vendors as needed; (b) the Village may retain certain existing subscriptions, hardware-as-a-service agreements, or warranties, which the successful Proponent must assume and administer; (c) the Village may, at its sole discretion, purchase hardware from sources other than the successful Proponent, provided the successful Proponent is given an equal opportunity to submit competitive pricing for that hardware, and any such supported hardware must still be onboarded, supported, and managed by the successful Proponent as part of the managed services arrangement; and (d) a secure credential management approach will be required (no shared spreadsheets of passwords).

Critical systems and dependencies to be addressed by proponents: Proponents must describe how they will support core municipal business systems, network connectivity between sites, Microsoft 365 identity and collaboration services, backup and recovery tooling, printers, copiers/MFDs, cell phones/mobile devices, and coordination with third-party software, telecommunications, and device vendors. Where assumptions are made due to incomplete inventory details, proponents must clearly list those assumptions and identify any information required from the Village during onboarding.

4. Scope of Work

4.1 Managed IT Services (Complete Coverage)

For clarity, the definition of "IT-related equipment" in Section 2 applies throughout this RFP and will apply to the resulting contract.

- Single point of contact and ticketing system for all IT incidents and requests.
- Remote support for end users and systems; onsite support as required.
- Proactive monitoring, alerting, and remediation for endpoints, servers, and network devices.
- Operating system and third-party patch management.
- Endpoint management (standard builds, onboarding/offboarding, encryption, local admin control).
- Server administration (hardware, virtualization if applicable, OS maintenance, capacity monitoring).
- Network administration (firewalls, switches, wireless, VPN, segmentation, firmware management).
- Microsoft 365 tenant administration (identity, email, Teams/SharePoint/OneDrive, security baselines).
- Backup/DR operations (monitoring, troubleshooting, restore support, and scheduled test restores).

- IT documentation (network diagrams, asset inventory, standards, procedures, vendor contacts).
- Managed support and inventory administration for all IT-related equipment, including desktops, laptops, printers, copiers/MFDs, cell phones/mobile devices, monitors, peripherals, network devices, and other technology assets used in municipal operations.
- Vendor management and support coordination for ISPs, telephony, printers, copiers/MFDs, cell phones/mobile devices, and application vendors.

4.2 Cybersecurity Services

The Village requires a security-first approach suitable for a municipal environment. Proponents must describe their security stack, operations, and how services are delivered (in-house vs. subcontracted).

- **Identity & Access:** MFA enforced for privileged and end-user access; conditional access policies where available; least-privilege administration.
- **Endpoint security:** Managed endpoint protection/EDR; device encryption; local admin controls; secure remote support tooling.
- **Email/security awareness:** Email filtering and anti-phishing controls; regular security awareness training and phishing simulations.
- **Vulnerability management:** Patch compliance reporting; regular vulnerability scans; remediation tracking.
- **Logging & monitoring:** Centralized alerting; defined incident response process with timelines and communication plan.
- **Backup resilience:** Ransomware-aware backups; immutable/offline protections where available; routine restore testing.

4.3 Backup and Disaster Recovery (BDR)

- Monitor all backup jobs and address failures within defined timelines.
- Maintain documented RPO/RTO targets for critical systems (to be validated during onboarding).
- Perform at minimum: quarterly test restore of representative data and annual disaster recovery exercise (tabletop and/or technical test), with written results and recommendations.
- Provide clear procedures for emergency recovery, including escalation contacts available 24/7.

4.4 Onsite Support and Service Coverage

Proposals must include business-hours coverage (minimum 8:00 a.m. to 5:00 p.m., Monday to Friday, excluding statutory holidays) and after-hours coverage for critical incidents. Proponents must describe local onsite availability, travel charges (if any), and typical onsite response times for Keremeos. Onsite or remote consultation related to hardware advisory, lifecycle replacement, and budget planning is considered part of the standard managed services offering and is included in the fixed monthly managed services fees.

4.5 Governance, Change Management, and Asset/Configuration Management

- Maintain a current configuration management database or equivalent documented inventory for endpoints, servers, network devices, software licensing, warranties, and support contracts.
- Use a documented change management process for significant changes affecting production systems, including risk assessment, rollback planning, approval, maintenance windows, and post-change validation.
- Provide advance notice to the Village for planned maintenance or changes that may affect users, services, security controls, or integrations.
- Define account management and governance roles, including primary account manager, service manager, technical escalation lead, and security escalation contact.
- Maintain administrative access records with named-user accountability, least-privilege assignment, MFA, and timely removal of privileged access when no longer required.
- Support an annual review of asset lifecycle status, unsupported systems, licensing risks, and key technology dependencies, with written recommendations for remediation or replacement.

5. Service Levels (SLA) and Reporting

Priority	**Example**	**Target Response**	**Target Restore/Workaround**
P1 Critical	Municipal operations stopped; security incident; core network outage	15 minutes	4 hours (or best-effort continuous work until stable)
P2 High	Multiple users impacted; major system degradation	1 hour	1 business day

P3 Normal	Single user impacted; non-critical issue	4 business hours	3 business days
P4 Low/Request	Moves/adds/changes; minor requests	1 business day	As scheduled

Reporting requirements: Proponents must provide sample reports and commit to a monthly service report including ticket metrics, patch compliance, backup status, security events, and recommendations. The Village requires a minimum quarterly service review meeting and an annual planning/budgeting review.

Incident communications and major incident management: Proponents must describe how major incidents will be managed, including escalation to senior technical resources, communication intervals to the Village during active incidents, post-incident summary reporting, root-cause analysis for significant events, and tracking of corrective actions to closure.

5.1 Minimum Deliverables and Review Cadence

- **Monthly:** Service report (ticket volumes by priority, response/resolution performance, patch compliance, backup success/failures, security alerts/incidents, and recommendations).
- **Quarterly:** Service review meeting including risk register review, major incidents, lifecycle status, and upcoming project recommendations.
- **Annually:** IT roadmap/budget planning workshop; annual account security review; annual disaster recovery exercise report (or equivalent test), including results and remediation plan.
- **Ongoing:** Maintain current network diagram(s), asset inventory, administrative access list, vendor list, and operating procedures; provide updates upon material changes.

6. Privacy, Confidentiality, and Compliance

- Proponents must demonstrate knowledge of and ability to support compliance with BC FIPPA and municipal privacy obligations.
- Proponents must describe where data is stored/processed (including any subcontractors and security operations centres) and how privacy and confidentiality are protected.
- Personnel with access to Village systems must be subject to background screening appropriate to municipal work; describe your screening approach.
- Proponents must maintain strict confidentiality of all Village information and confirm their ability to comply with the security incident notification and reporting

timelines set out in Section 13.4, including notice within [twenty-four (24)] hours of discovery, an initial written summary within [one (1) business day], and a final incident report within [five (5) business days], unless otherwise agreed by the Village.

- Credential handling must use an approved secure method (vaulting, role-based access, audit trails, MFA).

6.1 Data Residency, Subprocessors, and Access Location

- Proponents must list all third parties/subcontractors (subprocessors) that may access Village systems or information and describe what access they have.
- Proponents must disclose the physical location(s) from which support will be delivered and where any service data, logs, backups, or documentation will be stored and processed.
- The successful Proponent must not add or change subprocessors that access Village information without providing advance notice and obtaining the Village's written approval (not to be unreasonably withheld).

6.2 Records, Freedom of Information, and Retention Support

- Proponents must acknowledge that the Village is subject to access-to-information and records obligations. Proposals and contract deliverables may be considered records of the Village.
- Where the Proponent marks information as confidential, it must clearly identify the specific portions and the reasons; however, the Village may still be required to disclose information in accordance with applicable law.
- Proponents must describe how they will support retention requirements for email, documents, and backups (e.g., retention policies, eDiscovery support, legal hold processes where applicable).

7. Transition, Onboarding, and Knowledge Transfer

Proponents must provide a detailed transition plan that minimizes disruption to municipal operations. The Village expects onboarding to include (at minimum):

- Kickoff meeting and confirmation of governance, contacts, escalation paths, and change approval process.
- Current-state assessment and validation of asset inventory, including desktops, laptops, printers, copiers/MFDs, cell phones/mobile devices, network equipment, licensing, warranties, subscriptions, and related support arrangements.
- Documentation creation/updates: network diagrams, admin access map, vendor list, backup/DR procedures, standards.

- Deployment or validation of management agents/tools (monitoring, remote support, patching, security).
- Microsoft 365 tenant review and security baseline implementation (MFA/conditional access, admin roles, auditing).
- Backup/DR review, test restore, and remediation plan for any gaps.
- Handover from outgoing provider, including secure transfer of credentials and documentation.

8. Proponent Qualifications and Minimum Requirements

- Demonstrated experience delivering managed IT services for municipalities or public sector organizations of similar size and complexity.
- Ability to provide local onsite support in the South Okanagan, with stated travel policies.
- Service desk with ticketing, metrics, and escalation; describe hours and after-hours support model.
- Cybersecurity capability, including EDR/monitoring and incident response; identify any subcontractors.
- Documented quality assurance processes and customer satisfaction approach.
- At least three references (preferably municipal/public sector) with contact information.
- Proof of insurance: commercial general liability and professional liability/errors & omissions (minimum limits to be stated by the Village).
- Ability to provide documented business continuity for the proponent's own service operations, including backup coverage for key staff, continuity of support tools, and contingency plans if the proponent experiences an outage or cyber incident.

9. Submission Instructions

- **Submission delivery:** email to: operationsmanager@keremeos.ca, Attn: Don Bishop
- **Closing:** Proposals must be received before the Closing Date & Time. Late submissions may be rejected.
- **Questions:** Submit questions in writing to the Procurement Contact by the Questions Deadline.
- **Proposal validity:** Minimum 90 days from Closing Date.
- **Costs:** All costs incurred by Proponents are the Proponent's responsibility.

9.1 Procurement Rules and Conduct

- **Sole point of contact:** The Procurement Contact is the only authorized contact for this RFP. Contact with other Village staff, elected officials, or consultants regarding this RFP may result in disqualification.
- **Irregular proposals:** The Village may, at its sole discretion, waive minor irregularities, request clarification, or accept a proposal that does not strictly comply with the requirements.
- **Right to negotiate:** The Village may negotiate with one or more Proponents, including scope, pricing, and contract terms, without reissuing the RFP.
- **Partial award:** The Village may award all or part of the Scope of Work.
- **Conflict of interest:** Proponents must disclose any actual or potential conflicts of interest, including relationships with Village staff or elected officials.
- **Collusion:** By submitting a proposal, the Proponent represents that it has not communicated with any competitor for the purpose of restricting competition.

10. Proposal Content and Response Format

To be considered complete, proposals should be organized in the following order and clearly reference the corresponding section headings:

1. **Cover Letter** signed by an authorized signing officer.
2. **Company Profile** (ownership, years in business, office locations, number of staff/technicians, subcontractors).
3. **Proposed Service Model** (helpdesk, onsite support, escalation, account management, after-hours, and confirmation of how printers, copiers/MFDs, cell phones/mobile devices, and other IT-related equipment are included in service coverage).
4. **Technical Approach** (tools used for monitoring/RMM, ticketing, documentation, security operations).
5. **Cybersecurity Approach** (controls, monitoring, incident response, awareness training, reporting).
6. **Microsoft 365 Approach** (tenant admin, identity, backups, retention, best practices).
7. **Backup/DR Approach** (monitoring, test restores, annual DR exercise, ransomware resilience).
8. **Onboarding/Transition Plan** with timeline and responsibilities (Village vs. Proponent).
9. **Service Levels** (response/resolution targets, uptime assumptions, exclusions).
10. **Pricing** (see Section 12) including any optional add-ons.
11. **References** (minimum three).

12. **Exceptions** (any requested changes to contract terms or scope).
13. **Contract Term, Renewal, Notice, and Incident Timeline Confirmation** confirming acceptance of the Village's highlighted standard placeholders for initial term, renewal options, termination notice periods, transition-out assistance duration, and security incident notification/reporting timelines, or clearly identifying any requested exceptions.
14. **Assumptions and Dependencies Register** identifying any pricing or service assumptions, required third-party dependencies, unsupported conditions, and information the Proponent requires from the Village to finalize onboarding and steady-state support.

10.1 Mandatory Response Matrix

To support efficient evaluation, Proponents should include a response matrix that addresses each requirement in this RFP and identifies whether the requirement is fully met, partially met, or excluded, with a reference to the relevant page or appendix in the proposal. At minimum, the matrix should cover service desk coverage, onsite support model, cybersecurity controls, Microsoft 365 administration, backup/disaster recovery testing, reporting cadence, data residency and access location, subcontractors, transition approach, coverage for printers, copiers/MFDs, cell phones/mobile devices, and other IT-related equipment, pricing assumptions, contract term and renewal acceptance, termination notice periods, security incident notification and reporting timelines, and any contract exceptions.

11. Evaluation Process and Criteria

The Village intends to evaluate proposals to determine best overall value. The Village may shortlist Proponents for interviews and/or request clarifications.

Criteria	**Suggested Weight**
Understanding of requirements and completeness of response	15%
Service model, local support, governance, and SLAs	20%
Cybersecurity capability, privacy compliance, and incident response approach	20%
Technical approach, tools, documentation, reporting, and lifecycle planning support	15%
Municipal/public sector experience, references, and local capacity	10%

Transition readiness, contract exceptions, and risk to the Village	5%
Pricing and overall value	15%

12. Pricing and Cost Proposal Requirements

Provide pricing in Canadian dollars (CAD), excluding GST. Pricing must clearly distinguish between (a) fixed monthly managed services, (b) hourly/project rates, and (c) pass-through licensing/hardware costs. Identify any minimum terms, onboarding fees, and travel charges. Pricing should remain firm for the initial contract term of [three (3) years], unless otherwise clearly identified by the Proponent in its assumptions, exclusions, or requested contract exceptions. The Village may, at its sole discretion, purchase hardware from other sources, provided the Proponent is given an equal opportunity to submit competitive pricing for that hardware.

A. Fixed Monthly Managed Services	
Per-user managed services fee (describe inclusions)	$/user/month
Per-device managed services fee (if applicable)	$/device/month
Minimum monthly charge (if any)	$
Included onsite visits (frequency and hours)	
B. One-Time and Project Fees	
Onboarding/transition fee (if any)	$
Standard hourly rate (business hours)	$/hour
After-hours hourly rate	$/hour
Project management rate (if different)	$/hour
C. Licensing and Security Add-ons (itemize; can be Village-paid direct or partner-resold)	
Microsoft 365 licensing management fee (if any)	$
Endpoint security/EDR/MDR (per user or device)	$
Microsoft 365 backup (per user)	$
Security awareness training/phish testing	$

13. Contract Terms (Summary)

- **Term:** The Village anticipates an initial contract term of [three (3) years], with up to [two (2)] optional renewal terms of [one (1) year each], exercisable at the Village's sole discretion and subject to satisfactory performance, pricing, and annual budget approval.
- **Non-exclusive:** The Village may obtain services from others as it deems necessary.
- **Right not to award:** The Village is not obligated to accept any proposal and may cancel this RFP.
- **Confidentiality:** Proponents must keep all Village information confidential.
- **Subcontracting:** Must be disclosed and subject to Village approval; Proponent remains responsible.
- **Insurance:** Successful Proponent must provide proof of required insurance prior to award.
- **Indemnity and limitation of liability:** To be negotiated in final agreement; Proponents must identify exceptions.
- **Freedom of Information:** Submissions may be subject to access requests; mark proprietary sections clearly.

13.1 Ownership of Data, Accounts, and Documentation

- All Village data, configurations, documentation produced for the Village, and administrative credentials are and remain the property of the Village.
- Upon request, the Proponent must provide the Village with a current export of documentation, asset inventory, and configuration backups in commonly used formats.
- All accounts must be created and maintained under Village ownership (e.g., Village-controlled tenant ownership and administrative accounts), not under the Proponent's master tenant.

13.2 Termination and Transition-Out Assistance

- **Termination for convenience:** The Village may terminate the agreement for convenience upon [sixty (60) to ninety (90)] days written notice. If the agreement permits termination by the Proponent for convenience, the Proponent must provide not less than [ninety (90)] days written notice and continue to provide uninterrupted services during the notice and transition period.
- **Termination for cause:** The Village may terminate for cause (including material breach or repeated failure to meet service levels) on notice and opportunity to cure, except where immediate termination is warranted.

- **Transition-out:** For a period of [thirty (30) to sixty (60)] days following notice of termination or expiry (or longer by mutual agreement), the Proponent must provide reasonable transition assistance at the rates in the Pricing section, including secure transfer of documentation, credentials, system knowledge, and coordination with the Village or a replacement provider.
- **No lock-in:** The Proponent must not withhold passwords, documentation, or access to Village-owned systems for any reason other than lawful direction by the Village.

13.3 Audit Rights and Performance Management

- The Village may request reasonable evidence of performance against service levels, including ticket metrics, patch compliance, backup success rates, and security monitoring coverage.
- The Village may audit (or have a third party audit) the Proponent's compliance with material contract requirements related to Village systems and information, on reasonable notice, subject to confidentiality and security constraints.

13.4 Vendor Business Continuity, Insurance, and Security Incident Notification

- **Vendor continuity:** Proponents must describe their internal business continuity plan (staffing coverage, tool redundancy, and how services continue during outages affecting the Proponent).
- **Insurance:** The successful Proponent will be required to carry, at minimum, Commercial General Liability of $[2,000,000] per occurrence and Professional Liability / Errors & Omissions of $[1,000,000] per claim (or as otherwise specified by the Village). Proponents should indicate current coverage and ability to meet requirements.
- **Security incident notification:** The Proponent must notify the Village of any actual or suspected security incident involving Village systems or information without undue delay and in any event within [twenty-four (24)] hours of discovery, or sooner where the incident is actively affecting operations, confidentiality, integrity, or availability. The Proponent should also provide an initial written incident summary within [one (1) business day] of notification and a final incident report, including root cause and corrective actions, within [five (5) business days] or such other timeline agreed by the Village.

14. Appendices

Appendix A - Proponent Submission Checklist

- Signed cover letter
- Completed pricing template (Section 12)
- Service model and SLA commitments
- Cybersecurity approach and incident response
- Transition/onboarding plan
- References (minimum three)
- Insurance confirmation (current certificates or commitment to provide upon award)
- List of subcontractors (if any)
- Confirmation of acceptance, or requested exceptions, for the Village's highlighted placeholders for contract term, renewal options, termination notice periods, transition-out duration, and security incident notification/reporting timelines

Appendix B - Planning Context (Informational)

The Village maintains multi-year IT lifecycle planning. Proponents should be prepared to support annual budgeting and replacement planning. For context, prior planning materials anticipate combined operating and capital IT spending that varies year-to-year based on lifecycle replacements (e.g., increased costs in years with server and endpoint refreshes). Proponents should explain how they will support lifecycle planning, asset tracking, and budget forecasting.