# Request for Proposals

# End-to-End Cloud-Based IT Support Services

Submission Deadline: September 19, 2025, by 11:59pm. ET

## Background

The Association of Faculties of Medicine of Canada (AFMC), a registered charity, is seeking proposals from qualified IT Managed Service Providers (MSPs) to deliver comprehensive, cloud-native IT support. AFMC is a fully remote organization made up of 55 employees, operating a modern, serverless environment powered by Microsoft Azure and Microsoft 365.

Our users work exclusively with a mix of corporate and Bring Your Own Device (BYOD) Windows devices, Windows 365 virtual desktops, macOS, iOS, iPadOS, and Android endpoints.

Our help support ticket volume is generally on the low side; monthly activity can vary and at times drop to zero. This underscores the importance of a managed support model focused on proactive maintenance, dependable availability, and cost-effective service rather than high-volume responsiveness.

We are looking to build a proactive, responsive, Service Level Agreement (SLA)-driven partnership with a vendor that can scale alongside our continued growth, while ensuring robust security, regulatory compliance, and high user satisfaction based on exceptional customer service.

## Scope of Work

The selected vendor will be responsible for providing end-to-end IT support services, including but not limited to:

- Provide comprehensive helpdesk support for remote staff across Canadian time zones and, when needed, internationally—covering initial incident triage, routine service requests, escalation coordination, and advanced technical troubleshooting—in accordance with IT Service Management best practices aligned with ITSM best practices as defined by ITIL.
- Administration of Microsoft 365 services including Exchange Online, SharePoint, OneDrive, Intune, Teams, Defender and Microsoft Azure.
- User onboarding/offboarding, license assignment, and access provisioning via Microsoft Azure, Microsoft Entra and Action1.
- Endpoint management using Microsoft Intune, Endpoint Manager and Action1 (various OS)
- Device compliance enforcement and conditional access policies.
- Monthly security reviews and proactive recommendations.
- Quarterly SLA performance reporting, business reviews and roadmap discussions.
- Incident response for account compromise or service interruption.
- Support for Windows 365 configuration and troubleshooting.
- Organization wide password management setup.
- Ongoing monitoring, alerts, and health reports for Microsoft 365 and Azure services.

- AFMC Internet Registrars, renewing, maintaining, monitoring and implementing Domain Name Services routings.
- Coordinate and act on behalf of AFMC all hardware / technology solution purchases.

**Appendix A** – Detailed Responsibilities is attached with a comprehensive breakdown of duties and expected SLAs

## Experience & Knowledge

The selected proponent must demonstrate:

- Proven experience supporting remote-only Microsoft 365 and Azure environments.
- Expertise with Intune, Microsoft Defender, conditional access, and Azure AD.
- Experience with cross-platform (Windows/macOS) environments.
- Security certifications or credentials (e.g., MS-500, SC-900).
- Experience supporting Windows 365.
- Experience in providing support on a variety of technology solutions (Box.com, Spam management, phishing user testing, helpdesk management, video – voice conferencing, Google Workspace, Amazon Web Services – data storage, Microsoft Azure Database hosting).

## Budget & Schedule

The budget should reflect a monthly managed services fee for supporting approximately 55 users, plus optional per-hour rates for projects or escalations beyond scope.

The agreement will have an initial term of one year, renewable annually. AFMC reserves the right to initiate a new Request for Quotation (RFQ) process every three years to ensure ongoing value, performance, and alignment with organizational needs and industry best practices.

Budget submissions should be itemized, presented in Canadian dollars, cover all costs, and separately list all applicable taxes. Note that budget information should be limited to 1 section only, not weaved throughout the proposal.

## Cyber Liability and Insurance Coverage

The respondent must disclose details of any Cyber Liability Insurance and Technology Errors & Omissions (Tech E&O) coverage currently held, specifically as it relates to the delivery of Azure and Microsoft 365 management services. This should include:

- Insurance provider and coverage limits
- Proof of current Cyber Liability and Tech E&O coverage
- Confirmation of coverage scope relevant to Microsoft 365 and Azure services
- Agreement to maintain coverage throughout the engagement
- Agreement to inclusion of indemnification provisions within the contract to protect AFMC from vendor-related incidents

The selected vendor may be required to provide proof of insurance prior to contract execution and maintain coverage throughout the engagement.

## Rated Criteria

Submissions will be evaluated under the following criteria:

| Criteria | Weighting |
|---|---|
| **Relevant Technical Experience and Qualifications** *(incl. Certification, Microsoft Partner)*<br>*Assess the proponent's proven experience and qualifications in IT operations supporting multi-stakeholder environments, including collaboration across departments and service alignment.*<br><br>*Considerations: Relevant education, certifications and industry credentials; years of experience in related fields; suitable team qualifications, proven commitment to exceptional customer service.*<br><br>*Vendor's experience supporting cloud-native, serverless environments and remote workforces.*<br><br>*Experience managing mixed OS environments (macOS, Windows, Android, iOS)* | 20 |
| **Capacity to meet deliverables required**<br>*Assess the vendor's ability to deliver full IT support remotely and scale with future growth.*<br><br>*Considerations: Adequacy of team expertise and assigned roles; resource availability (staffing, tools, infrastructure); risk management and problem-solving capabilities.* | 20 |
| **Security & Compliance**<br>*Assess the proponent's ability to maintain strong security and compliance standards.*<br><br>*Considerations:*<br>*Familiarity with Canadian privacy regulations and healthcare data handling*<br>*Endpoint protection, identity management, and secure remote access*<br>*Incident response and reporting protocols*<br>*Method for SLA monitoring and client transparency (e.g., shared dashboards, reports)* | 20 |
| **Suitability**<br>*Assess the proponent's reputation and client success in similar environments.*<br><br>*Considerations: References from organizations with remote, cloud-native setups; Client retention and satisfaction metrics.* | 10 |
| **Pricing***<br>*Scored using relative pricing formula, see process documentation linked below for full details.*<br><br>*Considerations: Transparent pricing structure; Flexibility for scaling and service adjustments; Cost-effectiveness compared to competitors* | 25 |

| Criteria | Weighting |
|---|---|
| **Social Procurement**<br>*Assess the proponent's commitment to delivering social value through their organization or approach.*<br><br>*Considerations: Whether the proponent is a social enterprise or non-profit; demonstrated outcomes such as inclusive hiring, community benefit, or reinvestment into social missions.* | 5 |
| **Total Points** | **100** |

Submissions will be scored according to the following scale:

| Point Scoring Key | Score |
|---|---|
| **Unresponsive** - No response is provided or the response is not relevant to the question/criteron | **0** |
| **Poor** - The response siginificantly fails to meet the standards required, contains significant shortcomings, and/or is inconsistent with expectations | **1** |
| **Unsatisfactory** - The response falls short of achieving the expected standard in a number of identifiable respects | **2** |
| **Satisfactory** - The response meets the requirement in certain material respects and provides certain information which is relevant, but is lacking or inconsistent in material respects | **3** |
| **Good** - The response meets the requirement in most material respects but is lacking or inconsistent in some minor respects | **4** |
| **Excellent** - The response meets the requirement in all material respects and is extremely likely to deliver the required output/outcome | **5** |

## Proposal Submission Instructions

Proposals should be sent to the RFP Administrator, Angela Kojok at akojok@afmc.ca by the deadline listed at the top of this RFP.

A rectification period of three (3) business days will follow the submission deadline, during which proponents may address non-substantive issues (e.g., missing signatures, formatting, or overlooked documents) identified by the RFP Administrator. No changes to core content or pricing will be permitted.

Requests for additional information may be directed to the above contact.

Questions or requests for clarification may be directed to the RFP Administrator. Early confirmation of intent to submit is appreciated; proponents who do so will receive any updates issued during the open period.

This request for proposals is subject to the process, terms and conditions available here: https://www.afmc.ca/wp-content/uploads/2023/02/AFMC-RFP-Process-Terms-and-Conditions.pdf

Elements to include in the proposal:

- The proposal must be submitted in English as a PDF and should not exceed 15 pages in length. Pages beyond this limit will be removed and not provided to the evaluation team.
- The budget must be presented as the final section of the proposal and should not be included or referenced within other sections.
- Company overview and relevant experience
- Microsoft partner status
- SLA guarantees and clearly defined escalation and response procedures
- Key personnel and certifications
- Client references for similar environments
- Sample reports and onboarding documentation
- Proposed ticketing and reporting tools
- Social value-added services or enhancements
- At least 3 similar client references.
- Completed RFP Acknowledgement Form

# Appendix A

*Detailed Responsibilities with a comprehensive breakdown of duties and expected SLAs:*

## Detailed Responsibilities

The Service Provider shall provide the following capabilities:

**I. Endpoint & Desktop Support**

- Setup and configure AFMC assigned Windows, Apple or Android devices.
- Maintain OS and desktop software version compliance
- Provide tiered technical support, consistent with IT Service Management best practices as outlined by ITIL, for end users via email, phone, and remote desktop tools.
- Troubleshoot and resolve software and hardware issues
- Perform remote diagnostics and performance tuning
- Track and resolve tickets using a professional ticketing system (must support SLAs and reporting).
- Enroll and manage devices using Microsoft Intune for both Windows and macOS.
- Deploy and manage updates, patches, and apps via Intune/Endpoint Manager (Action1).
- Implement Conditional Access policies based on risk, location, and device health.
- Minimal support HappyFox ticketing system.
- Provide additional support to a small group of staff and occasional external partners using approved personal computers, including Windows 365 virtual machines.

**II. Microsoft 365 & Azure Cloud Services**

- Administer Microsoft 365 tenant: Exchange, SharePoint, OneDrive, Teams (including video / voice conferencing support).
- Manage Azure AD / Microsoft Entra ID: identity, roles, group policies.
- Support Microsoft Intune for device and app management.
- Provide Microsoft Defender support (endpoint, identity, cloud).
- Deploy and manage Multi-Factor Authentication (MFA).
- Manage licensing, renewals, and compliance.
- Provide Teams / SharePoint site, user access, and permissions management (Note: AFMC role base access utilizes Teams sites / channels are assigned access / maintain by the Teams owners).
- Manage Exchange Online settings, transport rules, safe senders/block lists, and spam filtering, with user access to quarantined emails.
- Ensure compliance with Microsoft security best practices and feature configurations.

**III. IT Asset Procurement & Lifecycle Management**

- Procure, configure, and ship IT equipment to remote users.
- Receive returned equipment from offboarding or device swap scenarios.
- Prepare returned devices for outgoing users, including wiping, reimaging, performing quality checks prior to redeployment, and updating asset tracking systems.
- Remotely wipe or retire lost/stolen devices in accordance with AFMC security policy.
- Maintain and provide access to reports on asset inventory of hardware, software, and associated licenses to maintain inventory accuracy and accountability.
- Track warranty, lifecycle, and refresh schedules.
- Assist AFMC by providing guidance and support in procuring the necessary licenses.

**IV. User Lifecycle: Onboarding & Offboarding**

- Provision new users with accounts, access, and equipment.
- Removing a user's access to systems, applications, and data for users securely and recover assets (deprovisioning).
- Manage identity and access controls.
- Assist with orientation.

**V. Role Change Management & Access Adjustments**

- Implement IT changes when staff transition roles.
- Update user permissions, group memberships, and access policies across Microsoft 365 and Azure AD.
- Reassign or revoke licenses, apps, and device profiles as needed.
- Ensure compliance with identity and access management protocols.
- Provide documentation and audit trail of role-based changes.
- Coordinate with the People, Culture and Excellence (PCE) team with new responsibilities.

**VI. Backup, Restore & Data Retention**

- Provide, configure and monitor cloud-based backup solutions.
- Ensure compliance with AFMC retention policies.
- Perform scheduled restore tests and biannual audits.
- Provide disaster recovery support and documentation.

**VII. Cybersecurity & Compliance**

- Support AFMC cybersecurity initiatives and awareness programs.
- Ensure endpoint and cloud compliance with privacy standards.
- Monitor and report on security incidents and vulnerabilities.
- Provide patch management and threat detection services.

**VIII. Daily System Health Checks & Monitoring (Microsoft 365 & Azure)**

- Check endpoint health, antivirus status, and system alerts.
- Monitor backup success and verify restore points.
- Review ticketing system for unresolved or escalated issues.
- Check for pending OS and software updates.
- Validate and communicate performance of key services like Exchange and Teams.
- Monitor Microsoft 365 service health dashboard.
- Review Azure AD sign-in activity and access policy logs for any unauthorized access.
- Confirm Microsoft Defender alerts and Intune compliance.
- Monitor license usage and flag unassigned or near-capacity situations (such as OneDrive, SharePoint and Exchange usage versus maximum allowed).
- Submit daily summary reports or update dashboard.
- Report anomalies or service degradations and recommended actions.

**Support Coverage Matrix**

| Category | Description | Notes |
|---|---|---|
| **Microsoft 365 Services** | Includes Exchange, Teams, SharePoint, OneDrive, etc. | Full monitoring, administration, and reporting provided. |
| **Azure Services** | Infrastructure, identity, cloud-based hosting, resource management | Covered under scope; replaces traditional on-prem server functions. |
| **Third-Party SaaS Applications** | SAS, SPSS, Adobe Pro, etc. | Limited installation, access setup, basic configuration, software patching, and basic troubleshooting |
| **Integration Services** | Connecting third-party tools to Microsoft ecosystem | Support offered when integration impacts Microsoft 365 or Azure directly. |
| **Domain Registrar & DNS Services** | Domain registration, renewal, DNS record management, and monitoring | Responsible for DNS routing, record updates, and renewal reminders. |

**Third-Party Applications in Use (Inventory)**

The following applications are currently used within AFMC Each is managed under independent licensing and support agreements with their respective vendors:

- Action1
- Adobe Creative Cloud
- Adobe Pro
- Amazon Web Services (S3)
- Antidote
- Canva
- Cisco WebEx
- Clearwater
- Dilitrust
- DocuSign
- Grammarly
- GreenVelope
- Happy Fox
- IBM SPSS
- Keeper Security
- Member365
- Nvivo
- QuickBooks Online
- SAS Analytics Pro on Viya
- SendGrid
- SQL Server (MI)
- Microsoft SQL Server Management Studio
- Tableau
- Xoyondo
- Zoom

*Note: This list is subject to change and will be reviewed periodically to reflect updates in the organization's technology footprint.*

AFMC THE ASSOCIATION OF FACULTIES OF MEDICINE OF CANADA

## Support Availability

| Category | Details |
|---|---|
| Business Hours | Mon–Fri, 7:00 AM–5:00 PM EST |
| Emergency Support | 24/7 for Critical Incidents |
| Microsoft 365 Uptime | 99.9% SLA Guaranteed |

## Response & Resolution SLAs

| Severity | Description | Initial Response Time | Resolution/ Workaround Target |
|---|---|---|---|
| **Critical** | System-wide outage or security incident impacting majority users (e.g., system down, data breach) | 30 minutes (24/7) | 4 hours |
| **High** | Major functional disruption, affecting multiple users or core services (e.g., email failures, Teams outage, service unavailable, password reset, device malfunction) | 2 hours | 8 hours |
| **Medium** | Impactful issue with workaround, Single-user issue or non-critical problem (e.g. device issue) | 4 hours | 1 business day |
| **Low** | General requests, minor issues, or inquiries (e.g., software install, documentation request) | 1 business day | 5 business days |

* Escalations must be logged and followed up until final resolution

## Performance Expectations

| KPI | Target |
|---|---|
| **Backup Success Rate** | 100% daily |
| **Endpoint Compliance** | ≥ 95% |
| **Patch Deployment Success Rate** | ≥ 98% |
| **SLA Adherence on Tickets** | ≥ 90% |

| | |
|---|---|
| **License Utilization Monitoring** | Weekly review |

## Reporting Requirements

- Daily health check dashboard with immediate alerts for critical issues.
- Daily ticket updates: vendor must log and track all support incidents in a system accessible by AFMC upon request.
- Weekly operational reports (major issues and ongoing escalations, anticipated peaks or staffing concerns, etc).
- Monthly license utilization reports.
- Quarterly SLA reporting: the vendor will monitor SLA performance and submit a quarterly SLA compliance report—including all relevant ticket metrics and resolution times. AFMC reserves the right to audit vendor-reported SLA data, request raw ticket logs, and initiate escalation procedures if SLA breaches occur.
- Quarterly performance and strategic review meetings.

## Penalties & Remedies

- Missed SLA targets: service credits or apply a percentage deduction from the monthly fee
- Consecutive SLA failures (defined as three missed SLA targets within any rolling three-month period): Trigger a joint contract review and mutually agree on a remediation plan.
- Consecutive critical SLA failures (two critical breaches within any rolling quarter): AFMC may issue a 30-day cure notice; failure to remediate allows AFMC to terminate for cause.
- Termination notice: AFMC may terminate the agreement with 30 days' notice if remediation fails or repeated SLA breaches persist.