Request for Proposals: Managed IT Services

Managed IT Services Requirements

1. Purpose

CCRW is seeking proposals from qualified managed service providers to deliver core operational IT services that support a secure, reliable, and responsive technology environment for employees working across Canada.

CCRW currently relies on limited internal capacity for several operational IT functions. Through this RFP, CCRW intends to transition to a managed service model that provides consistent employee support, stronger cybersecurity oversight, improved documentation, and reliable service coverage across national operations.

The selected provider will be expected to deliver day-to-day operational support in the following areas:

- employee onboarding and offboarding;
- service desk and technical support;
- device provisioning and management;
- Microsoft 365 and identity administration;
- endpoint security;
- cybersecurity monitoring and incident response; and
- related documentation, reporting, and operational advice.

CCRW will retain ownership of technology strategy, organizational systems, Salesforce, digital products, and innovation initiatives. The managed service provider will deliver the operational services defined in this RFP, escalate decisions that affect strategy or organizational systems, and provide documented operational advice to CCRW's leadership in support of those broader priorities.

2. Organizational Environment

CCRW employs approximately 60 staff members who work across 11 office locations in Canada or remotely across Canada. Services will normally be delivered remotely, and routine office visits are not required. CCRW's technical environment is summarized in Appendix D.

3. Required Service Coverage

Regular employee support must be available Monday to Friday throughout CCRW's national operating hours:

10:00 a.m. Newfoundland Time to 2:00 p.m. Pacific Time

Proponents must demonstrate reliable coverage throughout this service window and identify the location and time zones of support personnel.

Services will normally be delivered remotely. Routine visits to CCRW offices are not required. Proponents must describe how equipment repair or replacement will be coordinated and priced when remote resolution is not possible.

4. General Provider Obligations

The provider must deliver the services in this RFP using qualified personnel, documented procedures, accessible support practices, and clear accountability. The provider must maintain accurate operational records, promptly escalate risks, report on service performance, disclose subcontractors and third-party tools, and support orderly transition at the beginning and end of the agreement.

5. Endpoint Lifecycle Services

The provider will manage employee technology throughout the employment and device lifecycle, including authorized onboarding and offboarding, device preparation and deployment, account and access changes, shipping and returns, monitoring, support, reassignment, and secure disposal.

- create, configure, disable, and remove accounts, licences, groups, roles, permissions, sessions, and authentication methods at authorized times;
- prepare, configure, enroll, secure, update, monitor, troubleshoot, repair, replace, wipe, reassign, and dispose of Windows devices through approved tools, including Microsoft Intune and Bitdefender;
- configure email, Teams, OneDrive, approved applications, shared resources, encryption, updates, and security policies;
- support initial employee setup, sign-in, assistive technology compatibility, and confirmation that required systems are working;
- coordinate device and peripheral shipment, recovery, warranty service, replacement equipment, and missing-asset escalation; and
- maintain current account, access, asset, licence, warranty, and device-history records.

CCRW will provide authorized requests, employee information, start or departure dates, roles, managers, and required access. Proponents must state the notice required for routine onboarding and explain how urgent or involuntary departures will be prioritized, completed, and confirmed.

6. Service Desk and Service Levels

The provider will operate an accessible remote service desk as the first point of contact for approved operational IT support. Support must be available by email, telephone, and online portal and must include remote troubleshooting, ticket prioritization, escalation, status updates, documented resolutions, employee satisfaction monitoring, and analysis of recurring issues.

The service desk must support accounts, passwords, multifactor authentication, computers and peripherals, Microsoft 365, Teams, SharePoint, OneDrive, connectivity, remote work, approved applications, device performance, printing, scanning, security alerts, and assistive technology compatibility. Proponents must disclose any limits on ticket volumes, support hours, request types, or usage included in the proposed fee.

At minimum, a critical incident includes a suspected or confirmed cybersecurity event with material organizational impact, an organization-wide outage, loss of access affecting a substantial number of employees, or another material operational disruption. Proponents must complete the service-level response table in Appendix B, including priority definitions, response and restoration targets, escalation and communication requirements, measurement methodology, exclusions, reporting, and proposed remedies for repeated failure.

7. Microsoft Cloud, Routine Security Monitoring, and Recovery

CCRW requires routine operational administration, security monitoring, incident response, and recovery support appropriate for a national non-profit organization of approximately 60 employees. The provider will administer CCRW's existing Microsoft, Bitdefender, and Avanan environment, including Microsoft 365, Entra ID, Intune, Exchange Online, Teams, SharePoint, OneDrive, endpoint protection, email security, identity and access controls, and Microsoft Backup.

- administer users, groups, licences, multifactor authentication, conditional access, privileged access, security settings, and device compliance;
- review routine security alerts during agreed service hours, including suspicious sign-ins, Bitdefender endpoint alerts, Avanan email-security alerts, device-compliance issues, and relevant configuration risks;
- maintain Bitdefender endpoint protection, Avanan email-security configuration, operating-system and application updates, and approved Microsoft security configurations;
- provide initial incident triage, account or device containment, prompt notification and escalation, recovery support, and incident documentation;
- administer Microsoft Backup, monitor backup status and failures, document coverage and retention, periodically test restoration, and support recovery when required; and
- provide regular operational security, incident, backup, and recovery reporting.

The base scope does not require a dedicated security operations centre, continuous 24/7 monitoring, managed detection and response, penetration testing, advanced threat hunting, a

separate security information and event management platform, or digital forensics beyond initial triage. Proponents may recommend additional security services, but each must be justified and priced separately. Proposals must identify monitoring tools and hours, incident-response availability, notification and escalation procedures, subcontractors, data-storage and processing jurisdictions, insurance coverage, and the provider's own security controls.

8. Pricing and Contract Term

Proponents must complete Appendix A. CCRW prefers predictable pricing without unreasonable limits on routine service desk use; all recurring fees, included volumes, assumptions, exclusions, optional charges, and annual adjustments must be disclosed.

CCRW anticipates an initial three-year agreement, subject to negotiation and approval. The agreement should include service levels, performance reviews, price adjustments, termination rights, return of CCRW information and access, end-of-term assistance, and confirmation of CCRW ownership.

9. Transition Requirements

The successful provider will lead a structured transition that avoids material interruption to employee support, device management, security monitoring, and recovery capability. Proponents must propose the methodology and schedule.

The transition plan must identify activities, milestones, staffing, information required from CCRW, responsibilities, risks, dependencies, costs, knowledge-transfer arrangements, stabilization support, and the date responsibility for each service will transfer.

Transition will be complete when CCRW accepts the agreed documentation, inventories, administrative-access records, support and escalation procedures, security and recovery responsibilities, open-issue register, and knowledge-transfer materials.

10. RFP Timeline

To support a clear and orderly procurement process, CCRW anticipates using the following timeline for this RFP. The dates are provided for planning purposes and may be adjusted by CCRW if required.

RFP Milestone	Target Date
RFP issued	Wednesday, October 21, 2026
Deadline for proponents' questions	Wednesday, November 4, 2026, at 4:30 p.m. Eastern Time

CCRW responses and any addenda issued	Monday, November 9, 2026
Proposal submission deadline	Wednesday, November 18, 2026, at 4:30 p.m. Eastern Time
Evaluation period	November 19–27, 2026
Preferred proponent selected	Wednesday, December 2, 2026
Contract negotiation and approval	December 3–18, 2026
Target service commencement	Monday, February 1, 2027

The final issued RFP will include confirmed dates and times for each milestone. If CCRW changes the schedule after issue, it will communicate the change through a written addendum.

11. Questions and Addenda

To ensure that all proponents have access to the same information, questions about this RFP should be submitted in writing by the deadline identified in the timeline. Questions must be directed to the CCRW contact named in this document.

Where CCRW determines that clarification or additional information should be shared more broadly, CCRW may issue written responses or addenda. Proponents are responsible for reviewing all information issued during the RFP process and ensuring that their proposals reflect any applicable updates.

12. Submission Instructions

To support a fair and consistent review process, proponents are expected to submit complete proposals electronically by the proposal submission deadline. CCRW may decline to review submissions received after the deadline.

Each submission should clearly identify the proponent's legal name, primary contact, contact information, and confirmation that the proposal will remain valid for at least 90 days from the submission deadline.

Please submit your application to Brianne Dallas, Project and Community Coordinator at bdallas@ccrw.org.

13. Proposal Format

Proposals must be clear and concise, respond in the order of this RFP, and include completed Appendices A, B, and C.

As part of the evaluation process, CCRW may request clarification, additional information, presentations, demonstrations, or interviews with one or more proponents. Any such request will be intended to help CCRW better understand the proposal and assess fit with CCRW's requirements.

14. Evaluation Criteria

CCRW will evaluate compliant proposals using the weighted criteria below.

Evaluation Area	Weight
Understanding of CCRW's needs and proposed service model	20%
Experience, qualifications, staffing, and references	15%
Service desk, coverage, service levels, and account management	20%
Routine cybersecurity, privacy, Microsoft Backup, and risk management approach	20%
Transition plan and implementation approach	10%
Accessibility and inclusive service delivery	5%
Pricing, transparency, and overall value	10%
Total	**100%**

CCRW is not required to select the lowest-priced proposal. The successful proposal, if one is selected, will be the proposal that CCRW determines provides the best overall value and the strongest fit for its operating environment, service expectations, and organizational priorities.

15. Contractual Privacy and Data Protection

The provider must use CCRW information only to deliver the contracted services and must comply with applicable privacy, confidentiality, and data-protection obligations.

The agreement must address data-storage and processing locations, authorized access, confidentiality, retention, disposal, incident notification, subcontractors, insurance, and the return, transfer, or secure destruction of CCRW information.

CCRW will retain ownership and appropriate administrative access to its information, accounts, configurations, documentation, licences, and data.

16. Accessibility and Inclusive Service Delivery

As a national disability inclusion organization, CCRW expects the selected provider to deliver services in a way that is accessible, respectful, responsive, and inclusive. This includes recognizing that employees may have different communication preferences, assistive technology needs, or access requirements when seeking IT support.

Proponents should explain how accessibility and inclusive service delivery will be built into the support model, including:

- accessible service desk communication options;
- support for employees who use assistive technologies;
- plain language employee instructions and support materials;
- accessible ticket portals and support processes;
- flexible support approaches for employees with different communication or access needs;
- staff training or experience related to disability inclusion and accessible customer service; and
- procedures for identifying and removing barriers in the support experience.

All written materials provided to CCRW employees should be clear, accessible, and suitable for digital use. Where practical, materials should be provided in editable formats so they can be reviewed, adapted, and maintained by CCRW over time.

17. References

Proponents should provide references that demonstrate experience with organizations of comparable size or complexity, distributed workforce needs, non-profit operating environments, or similar accessibility and security requirements.

For each reference, proponents should include the organization name, contact name, contact information, length of engagement, scope of services, and a brief description of the work performed. CCRW may contact references during the evaluation process.

18. CCRW Rights and Reservations

CCRW reserves the right, at its sole discretion, to:

- amend, suspend, cancel, or reissue this RFP;
- waive minor irregularities and request clarification, additional information, interviews, or demonstrations;
- accept, reject, or negotiate any proposal in whole or in part; and

- decline to award a contract or select the proposal CCRW determines provides the best overall value.

Issuing this RFP does not obligate CCRW to enter into an agreement. Proponents are responsible for all costs of preparing a proposal and participating in the evaluation process.

19. Contact Information

To maintain a consistent process, all communications regarding this RFP should be directed to the CCRW contact identified below. Proponents should not contact other CCRW employees, board members, or representatives about this RFP unless directed to do so by the named contact.

Contact: Brianne Dallas
Title: Project and Community Coordinator
Email: bdallas@ccrw.org

Appendices

Appendix A: Pricing Schedule

Proponents must complete the following schedule and add rows where necessary.

Pricing item	Unit or basis	Price	Assumptions, inclusions, and exclusions
Monthly managed service fee	Per employee, per device, combined, or fixed		
Transition and onboarding	One-time		
After-hours and critical incident support	Hourly or included		
Project and consulting work	Hourly or daily		
Licences, travel, shipping, and other charges	Specify		
Annual price adjustment	Method and maximum		

Appendix B: Service-Level Response Table

Priority	Definition	Initial response	Restoration or resolution target	Update frequency and escalation
Critical				
High				
Medium				
Low				

Appendix C: Mandatory-Requirements Checklist

Proponents must indicate compliance with every mandatory requirement below, cross-reference supporting proposal content, and disclose any exception or alternative. Appendix D describes the current environment; Appendix E is optional and is not a mandatory requirement.

Canadian Council on Rehabilitation and Work
1867 Yonge Street, Suite 906
Toronto, ON M4S 1Y5
1-800-664-0925
www.ccrw.org

Mandatory requirement	RFP reference	Comply	Proposal reference	Exception or alternative
National workforce and service-window coverage	Sections 2–3			
Remote service delivery and equipment repair or replacement coordination	Section 3			
Qualified personnel, procedures, records, reporting, and subcontractor disclosure	Section 4			
Endpoint onboarding, offboarding, device lifecycle, and notice requirements	Section 5			
Accessible multichannel service desk and supported request types	Section 6			
Ticket limits disclosure and completed service-level response table	Section 6 and Appendix B			
Microsoft cloud administration, Bitdefender and Avanan monitoring, incident response, Microsoft Backup, and recovery	Section 7			
Security exclusions, privacy, subcontractor, data-location, insurance, and optional-service disclosures	Sections 7 and 15			
Completed pricing schedule and full cost disclosure	Section 8 and Appendix A			
Transition methodology, schedule, responsibilities,	Section 9			

risks, and acceptance deliverables				
Submission format and completed Appendices A, B, and C	Sections 12–13			
Questions directed only to the named CCRW contact	Section 11			
Proposal cross-references and disclosure of exceptions or alternatives	Appendix C			

Appendix D: Technical Environment Inventory

- Microsoft 365, Entra ID, Intune, Exchange Online, Teams, SharePoint, and OneDrive;
- Bitdefender endpoint security, Avanan email security, and Microsoft Backup;
- organization-owned Windows computers; and
- accessibility-related hardware and assistive technologies, where required.

Appendix E: Optional Device Leasing or Device-as-a-Service

Proponents may submit an optional device leasing or device-as-a-service model. The option must describe equipment specifications, lease term, monthly cost, refresh schedule, warranty and repair coverage, replacement procedures, end-of-term ownership, early termination costs, return requirements, and data wiping or destruction procedures. Optional pricing must be presented separately and will not replace the requirement to support CCRW-owned devices.