Hamilton/Burlington Society for the Prevention of Cruelty to Animals (HBSPCA)

Request for Proposal

Managed Detection, Response, and Security Protection Services

RFP Number: RFP2026-ITMDR01
Date of Issue: September 7, 2026
Proposal Due Date: 11:59pm on October 30, 2026

Contents

A. INVITATION AND GENERAL INFORMATION

A.1 Invitation to Proponents

The Hamilton/Burlington SPCA (HBSPCA) invites proposals from qualified Managed Detection and Response (MDR) and Managed Security Services Providers (MSSPs) to deliver independent, 24/7/365 cybersecurity monitoring, threat detection, containment, incident response, and security governance services.

The HBSPCA seeks a security partner whose primary responsibility is protecting organizational identities, devices, systems, data, and cloud services. The selected vendor will operate independently from the HBSPCA's managed IT services provider and will provide direct reporting to the HBSPCA's CEO.

A.2 Organization Overview

The HBSPCA is a not-for-profit charitable animal welfare organization serving Hamilton, Burlington, and surrounding communities. The organization operates a primarily cloud-based technology environment centered on Microsoft 365 and supports a hybrid workforce, volunteers, donor management systems, animal shelter operations, veterinary services, telephony systems, and public-facing digital platforms.

The HBSPCA has adopted a governance model requiring independent security oversight and monitoring separate from operational IT support.

A.3 Proposal Submission Deadline

Proposals must be received no later than: **11:59pm on October 30, 2026**

Late submissions will not be accepted.

A.4 Inquiries and Communications

All inquiries must be submitted by email to: **Shelley May, ExecProgramAsst@HBSPCA.com**

Questions must be received by: **11:59pm on September 21, 2026**

Responses will be issued to all registered proponents.

A.5 Proposal Delivery Requirements

Electronic submissions in PDF format are preferred.

Submit proposals to: **Shelley May, ExecProgramAsst@HBSPCA.com**

Subject Line: **RFP2026-ITMDR01**

A.6 Contract Term

The HBSPCA anticipates:

- Initial term: Three (3) years, with a 120-day notice period to cancel by either partner
- Scheduled Engagement:
    - December 1, 2026, Transition Planning (December 1st to February 1st, 2027)
    - February 1st, 2027, Full Management Starts

The successful proponent shall be responsible for all transition activities and must implement the transition in a manner that minimizes operational impacts, with downtime limited to approved and acceptable levels.

A.7 Disclaimer

The HBSPCA reserves the right to:

- amend or cancel this RFP
- reject any or all proposals
- accept a proposal other than the lowest-priced submission
- request additional information from any proponent
- conduct interviews with shortlisted firms
- negotiate scope, fees, and contract terms
- award no contract if deemed appropriate

All costs incurred in preparing a proposal are the responsibility of the proponent.

All materials submitted become the property of the HBSPCA.

A.8 HBSPCA Partnership Investment Requirement

The successful proponent will be required to make an annual charitable contribution in support of the HBSPCA's **Unleash Love** campaign.

As a community-based charitable organization, the HBSPCA seeks to develop partnerships with service providers who share its commitment to animal welfare and community impact. The required contribution will form part of the contractual agreement with the successful proponent and will be finalized during contract negotiations.

While this contribution is not an evaluation criterion and will not influence the assessment of proposals, proponents should acknowledge their willingness to support HBSPCA's mission and fundraising efforts as a valued community partner.

B. OBJECTIVES

The HBSPCA seeks a provider capable of:

- Providing 24/7/365 threat monitoring and response
- Detecting and containing threats in minutes rather than hours
- Protecting Microsoft 365 identities and cloud resources
- Providing independent oversight of operational IT practices
- Improving HBSPCA's security posture through measurable controls
- Supporting regulatory, privacy, insurance, and governance obligations
- Identifying cost efficiencies and savings versus current system innovation
- Performing full audit on current system to identify gaps
- Delivering executive-level reporting and recommendations

C. SCOPE OF SERVICES

The successful vendor shall provide the following.

C.1 Managed Detection & Response

Continuous monitoring of:

- Entra ID (Azure AD)
- Microsoft 365
- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- End-user devices
- Firewalls and network edge devices
- Cloud applications and integrations

Required Service Levels

Service	Requirement
Monitoring	24/7/365
Alert Acknowledgement	Vendor to propose
Threat Containment	Vendor to propose
Escalation	Immediate for critical incidents
Incident Reporting	Real-time and post-incident

C.2 Identity Security Management

The vendor shall provide monitoring and protection against:

- Foreign login attempts

- Impossible travel events
- MFA fatigue attacks
- Unauthorized privileged role assignments
- Privilege escalation
- Credential compromise
- Token theft
- OAuth application abuse
- Suspicious administrator activity

C.3 Security Baseline Ownership

The vendor shall establish and maintain a documented security baseline including:

- Conditional access policies
- Multifactor authentication enforcement
- Administrative role management
- Privileged Identity Management recommendations
- Break-glass account procedures
- Secure score improvement targets
- Identity governance recommendations

Quarterly compliance validation will be required.

C.4 Email Security

Services shall include:

- Anti-phishing protection
- Business Email Compromise (BEC) monitoring
- DMARC implementation and monitoring
- SPF validation
- DKIM management

- Executive impersonation protection
- Domain monitoring

C.5 Endpoint Detection & Response

Vendor shall provide:

- Managed EDR services
- Threat hunting
- Malware investigation
- Ransomware detection
- Device isolation capability
- Containment authority under approved playbooks

C.6 Vulnerability Management

Vendor shall provide:

- Monthly vulnerability scans
- Risk prioritization
- Remediation recommendations
- Tracking and validation of corrective actions
- Reporting of unresolved critical vulnerabilities

C.7 Incident Response Retainer

Services shall include:

- Incident response planning
- Evidence preservation
- Digital forensics support
- Cyber insurance coordination
- PIPEDA breach assessment support

- Regulatory notification guidance
- Executive communications support

C.8 Security Awareness Program

- Security awareness training
- Phishing simulations
- Executive training sessions
- Annual staff training campaigns
- Reporting on participation and effectiveness

C.9 Penetration Testing

Vendor shall provide:

- Annual penetration testing
- External attack-surface reviews
- Executive summary reports
- Remediation roadmap

D. VENDOR QUALIFICATIONS

Mandatory Requirements

- Canadian operations
- Canadian data residency for log storage
- 24/7 Security operations centre operated directly by the vendor
- SOC 2 Type II and/or ISO 27001 certification
- Minimum five years providing MDR/MSSP services
- Microsoft 365 security expertise
- Cyber liability insurance

- Ability to support Canadian privacy regulations

References

- Provide three references:
    - Minimum two organizations between 40–150 users
    - Minimum one nonprofit or public-sector organization

E. REPORTING REQUIREMENTS

Monthly Reports

Include:

- Security incidents
- Threat trends
- Security scores
- Vulnerability metrics
- Open remediation activities

Quarterly Executive Reports

Presented directly to the CEO and designated representatives.

Reports shall include:

- Overall security posture assessment
- Compliance with established security baseline
- Independent evaluation of MSP compliance
- Strategic recommendations

Immediate Reporting

Critical incidents must be escalated immediately.

F. PROPOSAL SUBMISSION REQUIREMENTS

Proposals must include:

Corporate Information

- Legal name
- Corporate structure
- Office locations
- Years in operation

Service Model

- SOC location(s)
- Staffing structure
- Threat monitoring process
- Escalation methodology

Technical Approach

- Security architecture
- Monitoring tools
- Incident response methodology
- Sample reports

Pricing

- Monthly recurring fees
- Per-user pricing (if applicable)
- Incident response rates
- Penetration testing costs
- Onboarding costs

G. EVALUATION CRITERIA

Criteria	Weight
Security Capability	30%
Microsoft 365 Expertise	15%
Response and Containment SLAs	15%
Experience and References	10%
Reporting and Governance	10%
Incident Response Capability	10%
Cost	10%

H. EVALUATION PROCESS

H.1 Evaluation Methodology

The Evaluation Committee will include representatives from our Senior Management Team.

The Evaluation Committee may:

- review and score submissions
- interview shortlisted proponents
- conduct reference checks
- request clarification or supplemental information

I. TIMELINE

September 7, 2026	RFP released
September 21, 2026	**Applicant inquiry period** concludes at 11:59pm. This period allows written contact with the HBSPCA to ask questions regarding the application and process. Questions may be submitted via email to Shelley May at ExecProgramAsst@hbspca.com. Emails should reference “RFP2026-ITMDR01 – Questions” in the subject line

October 30, 2026	**Proposals due** (emailed PDF preferred) by 11:59pm. Proposals submitted after this deadline will not be accepted
November 12-16, 2026	**Evaluation team reviews and scores** proposals and selects finalists
November 19-23, 2026	The **HBSPCA will notify finalists** by email. Finalist presentations will take place in-person or via Teams
November 26, 2026	**Awarding of contract**

J. NEGOTIATIONS AND AWARD

J.1 Negotiations

The HBSPCA reserves the right to negotiate with the preferred proponent regarding:

- scope of services
- fees
- staffing
- deliverables
- contract terms

Failure to reach mutually acceptable terms may result in negotiations with an alternate proponent.

J.2 Contract Award

No contractual relationship shall exist until a written agreement has been executed by both parties.