



CENTRE FOR ANALYTICS, INFORMATICS AND RESEARCH (CAIR)

REQUEST FOR PROPOSALS

FOR

CYBERSECURITY UPGRADE AND MANAGED SECURITY SERVICES

Request for Proposal Number: **RFP-039-26**

Issued: **July 21, 2026**

Submission Deadline: **Thursday, August 20, 2026 @ 10:00 AM NDT**

Request for Proposal			
Title:	Cybersecurity Upgrade and Managed Security Services		
Open Call #:	RFP-039-26	Issue Date:	July 21, 2026
Questions Deadline:	72 hours prior to close time	Closing Date and Time: Proposal Submission Format: Opening Date and Time:	Thursday, August 20, 2026 @ 10:00 AM NDT opencalls@mun.ca Thursday, August 20, 2026 @10:30 AM NDT Via Conference Line: 1-416-915-6530 (toll free) Access Code: 2771 253 1254 Attendee ID: Please Press Pound (#)
Proposals Irrevocable Period after Submission Deadline:			90 days
Proposal Submission: Responses to this solicitation must be submitted by email to opencalls@mun.ca. Email subject line must read: <u>RFP-039-26 CYBERSECURITY UPGRADE AND MANAGED SECURITY SERVICES</u>.			
Inquiries and Communication:			
Inquiries and communication: Strategic Procurement Office, Financial and Administrative Services, Memorial University of Newfoundland, opencalls@mun.ca . Inquiries accepted only via email. No phone calls will be accepted. Please reference <u>RFP-039-26 CYBERSECURITY UPGRADE AND MANAGED SECURITY SERVICES</u> in subject line. Emails not containing this requirement information on the subject line will NOT be responded to. Proposals submitted by fax, mail, courier, drop-off or by any other means of delivery other than by email stated above shall not be accepted.			

ABOUT MEMORIAL UNIVERSITY

As Newfoundland and Labrador's only university, Memorial has a special obligation to the people of this province. Established as a memorial to the Newfoundlanders who lost their lives on active service during the First and Second World Wars, Memorial University draws inspiration from these shattering sacrifices of the past as we help to build a better future for our province, our country and our world.

We are a multi-campus, multi-disciplinary, public university committed to excellence in teaching and learning, research and scholarship, and to public engagement and service. We strive to have national and global impact, while fulfilling our social mandate to provide access to university education for the people of the province and to contribute to the social, cultural, scientific and economic development of Newfoundland and Labrador and beyond.

The Memorial experience goes beyond academics; it invites a discovery of self, community and place. At Memorial, we celebrate our unique identity through the stories of our people – the work of scholars and educators, the ingenuity of students, the achievements of alumni – and the impact we collectively make in the province, the country and the world. Memorial is the natural place where people and ideas become.

At Memorial University more than 17,000 students from over 120 countries come together to discover. From the classics to advanced technology, Memorial offers certificate, diploma, undergraduate, graduate and postgraduate [programs](#) across [five campuses](#) and [online](#). A global network of over 110,000 accomplished [alumni](#) throughout the world strengthens Memorial University's capacity and reputation for leadership in [research](#), teaching and [public engagement](#). Read more [fast facts](#) about Memorial University.

Mission, Vision and Values

Vision

Memorial University will be one of the most distinguished public universities in Canada and beyond, and will fulfill its special obligation to the people of Newfoundland and Labrador.

Mission

Memorial University is an inclusive community dedicated to innovation and excellence in teaching and learning, research, scholarship, creative activity, service and public engagement.

Memorial welcomes and supports students and scholars from all over the world and contributes knowledge and expertise locally, nationally and internationally.

Values

Excellence: Encouraging and promoting excellence through innovation and creativity, rigor and pragmatism.

Integrity: Being honest and ethical in all interactions, maintaining the highest ethical standards in

teaching, research, public engagement and service.

Collegiality: Engaging others with respect, openness and trust in pursuit of a common purpose, having regard for individuals, ideals and the institution as a whole.

Inclusiveness and diversity: Embracing and acting on responsibility to guarantee diversity and equity.

Responsiveness: Being receptive to individuals and communities.

Accountability: Accepting responsibility for achievement of common goals and objectives.

Freedom and Discovery: Supporting the freedom to pursue knowledge that is based on individual and collective intelligence, curiosity, ingenuity and creativity.

Recognition: Acknowledging, tangibly, all aspects of university enterprise including teaching and learning, research, scholarship, creative activity and public engagement.

Responsibility to place: Valuing and fulfilling the special obligation to the people of Newfoundland and Labrador by supporting and building capacity for excellence that:

- addresses needs and opportunities for Newfoundland and Labrador;
- engages the university community on matters of national and international significance;
- produces and delivers academic programs of national and international caliber and,
- Recognizes the dynamic opportunities presented by a multi-campus institution.

Responsibility to learners: Recognizing students as a first priority and providing the environment and support to ensure their academic and personal success.

Interdisciplinary collaboration: Supporting overarching themes in all pursuits that cut across academic units and address significant opportunities and challenges for which Memorial is particularly well positioned to build nationally and internationally recognized capacity.

Sustainability: Acting in a manner that is environmentally, economically and socially sustainable in administration, academic and research programs.

Memorial's exceptional staff and students contribute to the vitality and positive environment of the university through active community engagement. Memorial University has always been a publicly engaged institution. Since the founding of the University in 1949, the work of many of Memorial's students, faculty and staff has emphasized the importance of strong, sustained partnerships with members of the public of Newfoundland and Labrador and beyond.

Faculty and Staff

Memorial is one of the largest employers in the province, with approximately 3,600 faculty and staff. Memorial has been recognized as an Employer of Distinction by the Newfoundland and Labrador Employers' Council, which is reflective of its investment in comprehensive benefits, services such as childcare and recreation facilities, emphasis on work-life balance, and its vibrant work environment.

Governance and Administration

The management, administration and control of the property, revenue, business and affairs of the University are vested in a Board of Regents. The Board is appointed under the *Memorial University Act* and is responsible for the management, administration, and control of the property, revenue, business and affairs of the university. Matters of an academic character are in general charge of the Senate of the University.

For more information on Memorial University of Newfoundland, please visit: Memorial home page:

<http://www.mun.ca/>

Territory Acknowledgements at Memorial:

We acknowledge that the lands on which Memorial University's Campus are situated are in the traditional territories of diverse Indigenous groups and we acknowledge with respect the diverse histories and cultures of the Beothuk, Mi'kmaq, Innu, and Inuit of this province.

PART 1 – SUBMISSION INSTRUCTIONS

1.1 Proposals to be Submitted on Time

Proposals must be submitted as set out above on or before the Submission Deadline. Proposals submitted after the Submission Deadline will be rejected. Onus and responsibility rests solely with the proponent to submit its Proposal to the email indicated in the Request for Proposal on or before the Submission Deadline. The Owner does not accept any responsibility for any proposals submitted by means other than the email listed above. Proponents making submissions near the deadline do so at their own risk due to server availability. The time for the closing will be determined according to the inbox time stamp on opencalls@mun.ca. Proposals received after the closing time based on this time stamp, will NOT be considered.

1.2 Proposals to be Submitted in Prescribed Format

Proponents should submit **One (1)** email submission as a single file in PDF format. Please note: File size cannot exceed 15 MB. Otherwise, server may reject proposal submission due to size. Proposals submitted by fax, mail, courier, drop off or by any other means of delivery other than by email stated above shall not be accepted.

1.3 Amendment of Proposals

Proponents may amend their Proposals after they have been submitted if, and only if, the amendment is emailed prior to the Submission Deadline marked **PROPOSAL SUBMISSION AMENDMENT followed by RFP-039-26 CYBERSECURITY UPGRADE AND MANAGED SECURITY SERVICES**. Proposal revisions, changes and alterations may be made only by completing a new proposal. Previous submissions will be cancelled and the submission with the most recent date and time will be considered the final proposal.

Email inquiries and requests for clarification shall be accepted up to **72 hours** prior to the closing time. Inquiries and requests for clarification received after this date shall not be addressed. The Strategic Procurement Office will be the only official source of information regarding this Open Call for Proposals and information from any other source shall be considered unofficial and may not be correct.

To ensure consistency and quality in the information provided to Proponents the Owner shall provide, by way of amendment to this request for proposals in the form of an addendum, any relevant information with respect to the Request for Proposal inquiries received in writing without revealing the source of those inquiries. Proponents are cautioned that it is their responsibility to ensure that they receive all information relevant to this Request for Proposal. The Owner shall not be responsible for Proponents who fail to inform themselves regarding the scope and nature of the work. The Owner shall publish all amendments on Memorial University's website at https://www.mun.ca/finance/strategic_procurement/ or current service providers: MERX: www.merx.com, Bids: www.bids.ca and PODS: www.pods.net. Proponents should check on a regular basis for Request for Proposal updates. Proponents are solely responsible for ensuring they are aware of and have complied with all amendments by proposal submission closing time. **In the event there is discrepancy between the service providers, MERX, Bids, and PODS and the https://www.mun.ca/finance/strategic_procurement/ website, the official website is https://www.mun.ca/finance/strategic_procurement/.** Proponents are welcome to register their email address through opencalls@mun.ca to receive addendum notifications from Open Calls as a matter of courtesy. This does not relieve any Proponent of their responsibility to ensure all addenda has been received.

1.4 Withdrawal of Proposals

Proponents may withdraw their Proposals prior to the Submission Deadline. To withdraw a Proposal, a notice of withdrawal must be sent to the opencalls@mun.ca prior to the Submission Deadline and must be signed by an authorized representative of the Proponents. The Owner is under no obligation to return withdrawn Proposals.

1.5 Proposals Irrevocable after Submission Deadline

Proposals shall be irrevocable for a period of **90** days running from the moment that the Submission Deadline passes.

1.6 Delivery

Time is of the essence and delivery schedule(s) are legally binding. Memorial University reserves the right to assess penalties or cancel awards to Bidders who fail to meet the stated delivery or completion dates. Delivery of all materials and services must be DAP (delivered at place) or DDP (delivered duty paid (all locations) and local environs).

1.7 Signature

Memorial University, in consideration of section 11 of the Electronic Commerce Act, confirms its acceptance of electronic signatures, or other acceptable form of electronic consent, in satisfaction of the signature requirement for proposal submissions. The electronic form of signature or consent must be directly related to the relevant proposal submission at issue and must be reliable, in a manner as determined by Memorial University, for the purpose of identifying the person submitting the proposal response. By submitting a proposal under this process, the proponent confirms that the signatory has the appropriate and proper authority to bind the proponent to its submission, a confirmation upon which Memorial University relies in the processing of the proposal submission. **Proponents must complete Appendix B – Submission Form. Proposals received without Appendix B completed will be deemed non-compliant.**

1.8 Closure

In the event that the University is closed earlier than normally expected prior to a scheduled Request for Proposal closing for that day, or for the full day, the closing date for those Request for Proposal will be extended to the next business day for the University at the same time as listed originally.

1.9 Corporations Act

The Corporations Act of Newfoundland and Labrador requires that an extra-provincial company be registered before it begins or carries on business in the Province. If your company is not registered, please apply for the appropriate forms and procedures to:

Commercial Registrations Division Department of Government Services
PO Box 8700
St John's, NL Canada
A1B 4J6
Phone: 709-729-3317, Fax: 709-729-0232
Website: http://www.gs.gov.nl.ca/registries/companies/corp_art_inc.html

[End of Part 1]

PART 2 – EVALUATION AND AWARD

2.1 Stages of Evaluation

The Owner will conduct the evaluation of Proposals in the following stages:

2.2 Stage I – Mandatory Submission Requirements

Stage I will consist of a review to determine which Proposals comply with all of the mandatory submission requirements. Proposals that do not comply with all of the mandatory submission requirements as of the Submission Deadline will, subject to the express and implied rights of the Owner, be disqualified and not evaluated further. The submission form (**Appendix B**) must be completed. Submission without **Appendix B completed will be disqualified.**

2.3 No Amendment to Forms

Other than inserting the information requested on the mandatory submission forms set out in the Request for Proposal, a Proponent may not make any changes to any of the forms. Any Proposal containing any such changes, whether on the face of the form or elsewhere in the Proposal shall be disqualified.

Stage II will consist of the following:

2.4 Mandatory Technical Requirements

The Owner will review the proposals to determine whether the mandatory technical requirements as set out in **Appendix A** been met. Proposals that do not comply with all the mandatory technical requirements will, subject to the express and implied rights of the Owner, be disqualified and not evaluated further.

2.5 Rated Criteria

The Owner will evaluate each qualified proposal based on the rated criteria set out in **Appendix C.**

2.6 Selection of Proponent

After the completion of Stage II proponents will be ranked based on their total scores, all scores from will be added together and proponents will be ranked based on their total scores. Subject to the reserved rights of the Owner, the top-ranked proponent may be selected to enter into the Agreement in accordance with the following section.

Provincial suppliers, suppliers with a place of business in Newfoundland and Labrador, will be given provincial supplier preference provision. This mandates an allowance of ten percent for provincial suppliers for all procurement below trade agreement thresholds.

Please note, the supplier preference does not apply when the estimated value of the commodity is above the trade agreement threshold shown below.

Public Body	Thresholds			
	Goods	Services	Public Works	Lease of Space
Memorial University	\$139,000	\$139,000	\$347,400	\$100,000

2.7 Notification

Notice of selection by the Owner to the preferred supplier(s) shall be in writing.

2.8 Failure to Enter into Agreement

If a preferred supplier fails to satisfy the pre-conditions of award within fifteen (15) days of notice of selection, the Owner may, without incurring any liability, proceed with the selection of another proponent and pursue all remedies available to the Owner

2.9 Payment Terms

The University's standard payment terms are net 30 days after delivery of goods, or net 15 days after successful completion of installation as applicable. In the case of services, payment terms are also net 30 days after successful completion of the service. These terms shall also apply in the case of sub- contracted items. Prepayments will not be considered unless the supplier provides an irrevocable standby letter of credit, or the supplier provides a credit reference from its banker satisfactory to the Director of Financial and Administrative Services.

[End of Part 2]

PART 3 – TERMS AND CONDITIONS OF THE OPEN CALL PROCESS

3.1 Incorporated into Proposal

All the provisions of this Request for Proposal are deemed to be accepted by each Proponent and incorporated into each Proponents' Proposal. A Proponent who submits conditions, options, variations or contingent statements to the terms as set out in this Request for Proposal, either as part of its Proposal or after receiving notice of selection, unless otherwise indicated, may be disqualified. If a Proponent is not disqualified despite such changes or qualifications, the provisions of this Request for Proposal, including any agreement set out in will prevail over any such changes or qualifications in the Proposal.

3.2 Proponents to Follow Instructions

Proponents should structure their Proposals in accordance with the instructions in this Request for Proposal. Where information is requested in this Request for Proposal, any response made in a Proposal should reference the applicable section numbers of this Request for Proposal.

3.3 Proposals in English

All Proposals are to be in English only.

3.4 No Incorporation by Reference

The entire content of the Proponent's Proposal should be submitted in a fixed form, and the content of websites or other external documents referred to in the proponent's Proposal but not attached will not be considered to form part of its Proposal.

3.5 References and Past Performance

In the evaluation process, the Owner may include information provided by the Proponents references and may also consider the Proponents past performance or conduct on previous contracts with the Owner or other institutions.

3.6 Information in Request for Proposal Only an Estimate

The Owner and its advisers make no representation, warranty or guarantee as to the accuracy of the information contained in this Request for Proposal or issued by way of addenda. Any quantities shown or data contained in this Request for Proposal or provided by way of addenda are estimates only and are for the sole purpose of indicating to Proponents the general scale and scope of the Deliverables. It is the Proponents' responsibility to obtain all the information necessary to prepare a Proposal in response to this Request for Proposal.

3.7 Proponents to Bear Their Own Costs

The Proponent will bear all costs associated with or incurred in the preparation and presentation of its Proposal, including, if applicable, costs incurred for interviews or demonstrations.

3.8 Proposal to be Retained by the Owner

The Owner will not return the Proposal or any accompanying documentation submitted by a Proponent.

3.9 Trade Agreements

Proponents should note that procurements falling within the scope of the Canadian Free Trade Agreement and/or the Canada-European Union Comprehensive Economic Trade Agreement are subject to those trade agreements but that the rights and obligations of the parties will be governed by the specific terms of this Request for Proposal.

3.10 No Guarantee of Volume of Work or Exclusivity of Contract

The Owner makes no guarantee of the value or volume of work to be assigned to the successful Proponent.

3.11 Proponent to Review Request for Proposal

Proponents shall promptly examine all of the documents comprising this Request for Proposal, and

- (a) shall report any errors, omissions or ambiguities; and
- (b) may direct questions or seek additional information

in writing by email to the Request for Proposal contact on or before the Deadline for Questions. All questions or comments submitted by Proponents by email to the Contact shall be deemed to be received once the email has entered the contact's email inbox. No such communications are to be directed to anyone other than the Request for Proposal Contact, and the Owner shall not be responsible for any information provided by or obtained from any source other than the Request for Proposal Contact. The Owner is under no obligation to provide additional information. It is the responsibility of the Proponent to seek clarification from the Request for Proposal Contact on any matter it considers to be unclear. The Owner shall not be responsible for any misunderstanding on the part of the Proponents concerning this Request for Proposal or its process.

3.12 All New Information to Proponents by Way of Addenda

This Request for Proposal may be amended only by addendum in accordance with this section. If the Owner, for any reason, determines that it is necessary to provide additional information relating to this Request for Proposal, such information will be communicated to all Proponents by addenda. Each addendum forms an integral part of this Request for Proposal and may contain important information, including significant changes. Proponents are responsible for obtaining all addenda issued by the Owner. In the Submission Form (**Appendix B**), Proponents shall confirm their receipt of all addenda by setting out the number of each addendum in the space provided. Proponents who **fail** to acknowledge all posted addenda will be deemed non-compliant and disqualified.

3.13 Addenda and Extension of Submission Deadline

Any addendum added within four (4) calendar days of the Request for Proposals closing (Including on closing day) will extend closing by a reasonable period to be determined by Memorial University

3.14 Verify, Clarify and Supplement

When evaluating Proposals, the Owner may request further information from the Proponent or third parties to verify, clarify or supplement the information provided in the Proponent's Proposal. The response received by the Owner shall, if accepted by the Owner, form an integral part of the Proponent's Proposal.

3.15 Notification to Other Proponents

In accordance with section 30 of the *Public Procurement Regulations*, once the Agreement is awarded by the Owner, the outcome of the Request for Proposal will be publicly posted at Public Procurement Agency Website.

3.16 Debriefing

Unsuccessful Proponents may request a debriefing within ten (10) business days after the award has been posted. The request must be sent in writing to the Request for Proposal Contact. The intent of the debriefing information session is to aid the Proponent in presenting a better Proposal in subsequent procurement opportunities. The debriefing process is not for the purpose of providing an opportunity to challenge the procurement process or its outcome.

3.17 Supplier Complaint Process

If a Proponent wishes to register a complaint with respect to the Request for Proposal process, it should provide it in writing and within the parameters established by section 25 of the *Public Procurement Regulations*, as amended. The notice must provide a detailed explanation of the Proponent's concerns with the procurement process or its outcome, in addition to such other information as may be required by the *Regulations*. Proponents should note that these complaint procedures are separate and distinct from any dispute resolution processes that may be provided for under applicable trade agreements. If a Proponent wishes to dispute a matter under an applicable trade agreement, the Proponent must follow the process set out in the trade agreement.

3.18 Conflict of Interest

The Owner may disqualify a Proponent for any conduct, situation or circumstances, determined by the Owner, in its sole and absolute discretion, to constitute a conflict of interest.

The Owner reserves the right to disqualify any Proponent that in the Owner's sole opinion has an actual or potential conflict of interest or an unfair advantage or may permit the Proponent to continue and impose such terms and conditions, as the Owner in its sole discretion may require.

For the purposes of this Request for Proposal, the term "Conflict of Interest" includes, but is not limited to, any situation or circumstance where in relation to the Request for Proposal process, the Proponent has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to: (i) having, or having access to, confidential information of the Owner in the preparation of its Proposal that is not available to other

Proponents, (ii) communicating with any person with a view to influencing preferred treatment in the Request for Proposal process (including but not limited to the lobbying of decision makers involved in the Request for Proposal process), or (iii) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive Request for Proposal process or render that process non-competitive or unfair.

Proponents are required to disclose, to the Request for Proposal Contact, any potential or perceived conflict of interest issues prior to Request for Proposal closing date and time.

3.19 Disqualification for Prohibited Conduct

The Owner may disqualify a Proponent, rescind a notification of selection or terminate a contract subsequently entered if the Owner determines that the Proponent has engaged in any conduct prohibited by this Request for Proposal.

3.20 Proponents Not to Communicate with Media

Proponents must not at any time directly or indirectly communicate with the media in relation to this Request for Proposal or any agreement entered pursuant to this Request for Proposal without first obtaining the written permission of the Request for Proposal Contact.

3.21 No Lobbying

Proponents must not, in relation to this Request for Proposal or the evaluation and selection process, engage directly or indirectly in any form of political or other lobbying whatsoever to influence the selection of the successful Proponent(s).

3.22 Illegal or Unethical Conduct

Proponents must not engage in any illegal business practices, including activities such as Proposal-rigging, price-fixing, bribery, fraud, coercion or collusion must not engage in any unethical conduct, including lobbying, as described above, or other inappropriate communications; offering gifts to any employees, officers, agents, elected or appointed officials or other representatives of the Owner; deceitfulness; submitting Proposals containing misrepresentations or other misleading or inaccurate information; or any other conduct that compromises or may be seen to compromise the competitive process provided for in this Request for Proposal.

3.23 Past Performance or Past Conduct

The Owner may prohibit a supplier from participating in a procurement process based on past performance or based on inappropriate conduct in a prior procurement process, including but not limited to the following:

- (a) illegal or unethical conduct as described above;
- (b) the refusal of the supplier to honour submitted pricing or other commitments; or
- (c) any conduct, situation or circumstance determined by the Owner, in its sole and absolute discretion, to have constituted a Conflict of Interest.

In addition, the Owner may suspend the proposal privileges of a supplier regarding non-compliant

or substandard performance in accordance with section 26 of the *Public Procurement Regulations*.

3.24 Confidential Information of the Owner

All information provided by or obtained from the Owner in any form in connection with this Request for Proposal either before or after the issuance of this Request for Proposal:

- (a) is the sole property of the Owner and must be treated as confidential;
- (b) is not to be used for any purpose other than replying to this Request for Proposal and the performance of the Agreement;
- (c) must not be disclosed without prior written authorization from the Owner; and
- (d) must be returned by the Proponent to the Owner immediately upon the request of the Owner.

3.25 Confidential Information of Proponents

This procurement process is subject to the *Access to Information and Protection of Privacy Act, 2015* (ATIPPA, 2015). A Proponent must identify any information in its Proposal or any accompanying documentation supplied in confidence for which confidentiality is requested to be maintained by the Owner. The confidentiality of such information will be maintained by the Owner, except as otherwise required by law or by order of a court or tribunal. Proponents are advised that their Proposal will, as necessary, be disclosed, on a confidential basis, to advisers retained by the Owner to advise or assist with the Request for Proposal process, including the evaluation of Proposals.

The Proponent agrees that any specific information in its submission that may qualify for an exemption from disclosure under subsection 39(1) of the ATIPPA, 2015 has been identified in its submission. If no specific information has been identified it is assumed that, in the opinion of the Proponent, there is no specific information that qualifies for an exemption under the subsection 39(1) of the ATIPPA, 2015.

Contracting with the Owner is a public process. Information provided through this process will be disclosed when requested under the ATIPPA, 2015, except where disclosure of that information is harmful to the business' interests, as set out in the three-part test in the ATIPPA, 2015.

Information, including the financial value of a contract resulting from this procurement process, will be publicly released as part of the award notification process, in accordance with section 30 of the *Public Procurement Regulations*.

If a Proponent has any questions about the collection and use of personal information pursuant to this Request for Proposal, questions are to be submitted to the Request for Proposal Contact. Further information relating to subsection 39(1) of the ATIPPA, 2015 is provided in guidance documents available through the Office of the Information and Privacy Commissioner at <https://oipc.ni.ca/guidance/documents>.

3.26 Reserved Rights of the Owner

The Owner reserves the right to:

- (a) make public the names of any or all Proponents as well as Proposal price and value of contract;
- (b) make changes, including substantial changes, to this Request for Proposal provided that those changes are issued by way of addendum in the manner set out in this Request for Proposal;
- (c) request written clarification or the submission of supplementary written information in relation to the clarification request from any Proponent and incorporate a Proponent's response to that request for clarification into the Proponent's Proposal. This shall not be an opportunity for Proposal repair;
- (d) assess a Proponent's Proposal on the basis of: (i) a financial analysis determining the actual cost of the Proposal when considering factors including quality, service, price and transition costs arising from the replacement of existing goods, services, practices, methodologies and infrastructure (howsoever originally established); and (ii) in addition to any other evaluation criteria or considerations set out in this Request for Proposal, consider any other relevant information that arises during this Request for Proposal process;
- (e) waive formalities and accept Proposals that substantially comply with the requirements of this Request for Proposal;
- (f) verify with any Proponent or with a third party any information set out in a Proposal;
- (g) check references other than those provided by any Proponent;
- (h) disqualify a Proponent, rescind a notice of selection or terminate a contract subsequently entered if the Proponent has engaged in any conduct that breaches the process rules or otherwise compromises or may be seen to compromise the competitive process;
- (i) cancel this Request for Proposal process at any stage;
- (j) cancel this Request for Proposal process at any stage and issue a new Request for Proposal for the same or similar deliverables;
- (k) accept any Proposal in whole or in part; or
- (l) reject any or all Proposals;

and these reserved rights are in addition to any other express rights or any other rights that may be implied in the circumstances.

3.27 Limitation of Liability

By submitting a Proposal, each Proponent agrees that:

- (a) neither the Owner nor any of its employees, officers, agents, elected or appointed officials,

advisors or representatives will be liable, under any circumstances, for any claim arising out of this Request for Proposal process including but not limited to costs of preparation of the Proposal, loss of profits, loss of opportunity or for any other claim; and

- (b) the Proponent waives any right to or claim for any compensation of any kind whatsoever, including claims for costs of preparation of the Proposal, loss of profit or loss of opportunity by reason of the Owner's decision not to accept the Proposal submitted by the Proponent, to enter into an agreement with any other Proponent or to cancel this open call process, and the Proponent shall be deemed to have agreed to waive such right or claim.

3.28 Governing Law and Interpretation

These Terms and Conditions of the Request for Proposal Process (Part 3):

- (a) are intended to be interpreted broadly and independently (with no particular provision intended to limit the scope of any other provision);
- (b) are non-exhaustive and shall not be construed as intending to limit the pre-existing rights of the Owner; and
- (c) are to be governed by and construed in accordance with the laws of the Province of Newfoundland & Labrador and the federal laws of Canada applicable therein.

3.29 Facility Compliance Requirement

- (a) Equipment, power tools, instruments and appliances intended for use within Memorial University's facilities must comply with all regulatory requirements related to use and/or installation in University facilities. This includes but is not limited to certification/listing by recognized agencies, Pressure Vessel Act of Newfoundland and Labrador and similar.
- (b) Items provided related to this open call that receive power from the University's electrical system must be certified or listed for use within Canada by a recognized agency such as Canadian Standards Association (CSA) or Underwriter Laboratories Canada (ULC). A full list of agencies recognized by Memorial University is available upon request.
- (c) Equipment, tools, instruments and appliances that generate pressure may require registration as a pressure system with the Province of Newfoundland and Labrador. Compliance with the Boiler, Pressure Vessel and Compressed Gas Regulations under the Public Safety Act of Newfoundland and Labrador and the Boiler, Pressure Vessel, and Pressure Piping Code CSA B51:19 shall be demonstrated.
- (d) The vendor is responsible for all costs associated with ensuring the system is compliant with legislative requirements and for the application and registration processes. Field certifications may be considered but all costs and efforts for such scenarios are the responsibility of the vendor.

PART 4 - ENVIRONMENTAL HEALTH AND SAFETY REQUIREMENTS

Maintaining a healthy and safe environment for all members of the campus community, as well as visitors, is a priority with the University. This involves commitment from all sectors of the campus community and extends to outside agencies having occasion to come on campus to conduct business.

The following requirements will apply to all work undertaken by contractors and service personnel on any University property or for any work undertaken on behalf of the Owner.

4.1.0 Regulations, Codes and Standards

Contractors shall be familiar with and abide by provisions of various safety codes and standards applicable to the work performed and should refer to 1.21.5 of General Conditions:

1.21.5 The Contractor shall be completely responsible for the safety of the Work as it applies to protection of the public and property and construction of the Work.

The codes that must be followed and enforced for safety are:

- a) The National Building Code, Part 8, Safety Measures at Construction and Demolition Sites (Latest Edition);
- b) Canadian Code for Construction Safety (Latest Edition) as issued by the Associate Committee of the National Building Code;
- c) The Occupational Health and Safety Act of Newfoundland and Labrador (most current version) and Regulations.

In particular, strict adherence to the Provincial Occupational Health and Safety Act and Regulations and with the National Building Code of Canada, Part 8 is required

4.2.0 General Health and Safety Regulations

- a) Contractors/service agencies shall ensure that members of the campus community are not endangered by any work or process in which they may be engaged. Work areas shall be adequately barricaded, and if dust or fumes are generated, suitable enclosures shall be installed to contain such emissions.
- b) No material shall be stored in such a way as to obstruct walkways or represent a danger to pedestrian or vehicular traffic.
- c) Adequate protection shall be provided to prevent the possibility of goods falling from scaffolding or elevated areas. Areas where goods are being loaded or off loaded shall be barricaded or otherwise protected to prevent unauthorized entry. Appropriate warning signs must be posted.
- d) The work areas must be kept reasonably clean and free from debris which could constitute a fire hazard. Care must be taken to ensure that the work process does not activate fire alarm

detection devices. (Generation of dust and fumes can activate smoke detectors causing a false alarm).

- e) Due consideration shall be given to fire safety in buildings. Flammable goods must be kept away from sources of ignition. No work involving the use of open flame devices must be undertaken around flammable solvents or gases.
- f) Some University buildings contain asbestos and other hazardous materials. Do not alter or disturb any goods believed to contain asbestos goods (unless this is a duly authorized part of the project). Consult with University officials before proceeding with any work.
- g) Safety Data Sheets shall be procured for any hazardous product used on campus. Such sheets shall be made readily available for consultation as required under the Workplace Hazardous Materials Information System (WHMIS).

NOTE: The above requirements are not to be considered all-inclusive and are considered complementary to the safety requirements outlined in the agreement between the University and Supplier. Certain conditions and circumstances may require adherence to additional safety requirements.

As a general requirement, contract/service personnel are expected to conduct all work on campus in a professional and safe manner and to give priority to the safety and welfare of members of the campus community.

4.3.0 Contractor Safety Management

4.3.0 All Contractors and Subcontractors shall be required Workplace NL Certificate of Clearance.

4.3.1 All Contractors and Subcontractors are required to give the Owner written permission to approach Provincial regulatory authorities for applicable safety-related information on their respective firms.

4.3.2 The Contractor must also provide the following:

4.3.3 Memorial reserves the right to request and audit the full health and safety program of Contractors and Subcontractors and their associated documentation. This documentation may include, but not be limited to the following:

- (a) Health and Safety Program and/or Manual
- (b) Site Hazard Assessment
- (c) Letter of Assurance for Compliance (third party certification)
- (d) Applicable documented safe work practices;
- (e) Inspection reports and schedules;
- (f) Required employee safety training certifications and qualifications;
- (g) Updated list of OHS Committee and/or a worker health and safety representative, or workplace health and safety designate;
- (h) Proof of completion of the Owner's contractor safety orientation within the prior three years.

4.3.4 Memorial University reserves the right to refuse or cancel any contract with a Contractor that is not in compliance with Memorial's standards for Safety.

4.3.5 The University reserves the right to stop any work or portion of work where no documentation can be produced on site which identifies the hazards presented by a piece of work, safe work procedures for work or certification of employees performing work. The Contractor is liable for any costs incurred by affected parties associated with such a stoppage.

4.4.0 Access To Site

4.4.1 All Contractors and Subcontractors to be used in the execution of the Contract shall give advance notification of when they will be on site. Any work to be performed outside of Regular Time must have advance approval of the Owner.

Any discontinuation of the Work which causes a Contractor or their Subcontractors to suspend operations onsite will require the following:

- a) Contractor/Subcontractors shall notify the Owner of the stop work date.
- b) Contractor/Subcontractors shall ensure the site is left in a safe and secure condition.
- c) Contractor/Subcontractors shall ensure that locks and tags on mechanical and/or electrical systems are removed and, where necessary, replaced by the University.
- d) Contractor/Subcontractors shall not return to site without expressed prior permission from the Owner.

[End of Part 4]

APPENDIX A – SPECIFICATIONS & SCOPE

Introduction

Given the critical nature of CAIR's computing infrastructure and the sensitivity of its data assets, CAIR is seeking proposals from qualified vendors to design, implement, and support a holistic cybersecurity program aligned with Zero Trust principles and modern security best practices.

The selected vendor(s) will provide a comprehensive, integrated cybersecurity solution that is scalable and subscription-based and that enhances the objectives below.

Vendor Delivery Model

Bidders may propose one of the following:

- Single vendor providing all required services
- Prime vendor utilizing subcontractors or strategic partners

Notwithstanding the model proposed, bidders must designate one organization as the Prime Contractor. The Prime Contractor shall be solely responsible and accountable for all aspects of service integration and delivery, SLA compliance, contract performance, escalation management and the performance of any subcontractors or third parties engaged in the provision of services.

The proposal must clearly identify all participating organizations, their responsibilities and reporting relationships.

Objectives

- Secure private access to CAIR applications and HPC resources
 - Strengthen secure access controls for users regardless of location or device
- Identity governance and authentication controls
 - Enforce strict identity validation and device posture compliance
- Real-time data security monitoring and protection
 - Protect high-value data assets (databases, data lakes, HPC storage)
- Enterprise SIEM/SOAR providing integrated threat detection and automated response capabilities
 - Provide real-time threat detection and response
- Protection against lateral movement within internal environments
 - Prevent lateral movements within internal networks
- Continuous managed security services (24/7)
 - Establish ongoing monitoring and managed services
- Annual cybersecurity risk assessment and advisory services
 - Conduct annual cybersecurity risk assessments.
- Supports our longer-term journey to a protected B security compliance

- Ensure all systems, data flows and services support alignment with Protected B security requirements and control baselines as part of longer term planned security classification roadmap.

Project Scope

The scope of this project includes the deployment of integrated security technologies, processes, and managed services to enhance secure access, protect sensitive research data, strengthen identity governance, prevent lateral movement, provide real-time threat detection and response, and conduct recurring cybersecurity risk assessments.

The solution must be scalable to support high-performance computing (HPC) environments and research workloads while enabling secure collaboration across distributed users, devices, and partner institutions.

Although this request does not specify all requirements for a Protected B state, any solution implemented should be in alignment with a future Protected B state for on-premises HPC infrastructure.

Security Classification Pathway (Protected B)

CAIR data assets will not be 100% classified up to **Protected B** status in this security stance upgrade, but the proposed solution must align to the secure processing, storage and transmission of Protected B information in accordance with applicable Canadian federal and provincial security standards.

Bidders must demonstrate how their solution is in alignment with Protected B sensitivity, including, but not limited to:

- Strong identity assurance and access control
- Encryption of data at rest and in transit
- Comprehensive audit logging and monitoring
- Secure data handling, storage and disposal
- Personnel and operational security controls

Proposal Requirements and Content

Vendor Qualifications

- Executive summary
- Contracting Model (specify subcontractors, suppliers and/or partners and their respective responsibilities)
- Company profile(s)
 - Overview: name, structure, locations, history, number of employees, core competencies, future vision including product roadmap
 - Contact information
- Relevant experience with HPC or large research environments

- Demonstrated experience supporting environments handling Protected B information
- Case studies
- Security certifications
- Financial stability statement
- Proof of certifications
- References

Project Approach

- Implementation
- Team Resources
- Support
- Managed services
- Implementation timeline and milestones

Proposals

- Technical proposal
- Financial/Commercial proposal (separate)

Solution Requirements

Strategic Business Goals and Objectives Requirements

- Cost and contract duration options
- Hardware and software requirements (as required)
- Business hours, time zone and location
- Extra charges for after-hours support
- Payment options
- Limitations
- Termination options and constraints

Functional Requirements		
<i>Mandatory requirements for operational security (must comply):</i>		
DESCRIPTION	VENDOR RESPONSE	
	YES	NO
1. Managed Security Services – 24/7 SOC		
• 24/7 Security Operations Centre (SOC)		
• Incident detection and validation		
• Tier 1–3 analyst support		
• Incident escalation procedures		
• Defined SLAs for:		
○ Detection time		
○ Response time		
○ Containment time		
• Monthly reporting:		
○ Incident metrics		
○ Risk posture trends		
○ Threat landscape summary		
• Dashboards providing continuous visibility for real-time security monitoring		
• Provision of endpoint detection tools		
• Security Governance Framework		
○ Creation of an Incident Response Plan detailing Access Control, Notification and Escalation to be defined jointly based on SOC experience.		
○ CAIR proposes the following escalation protocol:		

▪ Tier 1 — SOC Monitor. SIEM/log aggregation, EDR telemetry, network IDS/IPS alerts, authentication logs, firewall/VPN logs. Available feedback on dashboards.		
▪ Tier 2 — SOC Pre-authorized automatic response. Short list of actions (to be jointly defined) for immediate response such as - isolate a single endpoint showing active malware/C2 behavior, block a malicious IP/domain at the perimeter, disable a single compromised user credential, etc. Notification to CAIR immediately after action taken (within 1 hr).		
▪ Tier 3 — SOC Notifies Only. Anything touching compute nodes, storage holding research data, identity systems beyond a single account, anything that could halt active research workloads. An urgent call to on-call person (15 min) at CAIR who will take action. Only SOC notification and advice.		
Notification to include: affected systems/assets, timeline of what's known, indicators of compromise, containment actions already taken, and what evidence has been preserved etc.		
• Ability to coordinate security incidents with designated CAIR personnel and Memorial University OCIO where required		
• Support for legal, privacy, regulatory and reporting obligations associated with cybersecurity incidents		
• Protected B alignment		
Any data from CAIR must be stored on Canadian servers within AWS Canada or Azure Canada servers for security purposes.		
2. Lateral Movement Protection		
• Micro segmentation of:		
○ HPC nodes		
○ Storage environments		
○ Administrative systems		
• Identity-based segmentation		
• East-west traffic inspection		

• Detection of (including but not limited to):		
○ Pass-the-hash		
○ Credential replay		
○ Unauthorized service-to-service access		
○ Other recommended detection options		
3. SIEM / SOAR – Integrated Threat Detection & Response		
• SIEM		
○ Centralized log ingestion from:		
▪ Firewalls		
▪ Endpoints		
▪ Servers		
▪ HPC nodes		
▪ Identity providers		
▪ Databases		
○ Real-time correlation		
○ Threat intelligence integration		
○ Custom rule creation		
○ High EPS scalability		
• SOAR		
○ Automated incident triage		
○ Playbook-driven response		

○ Automated containment actions (e.g., disable account, isolate host)		
○ Ticketing integration (e.g., CAIR ticketing system, ServiceNow API)		
○ Forensic evidence collection		
• Threat Detection		
○ Behavioral analytics		
○ Lateral movement detection		
○ Insider threat detection		
○ Ransomware detection		
4. Annual Cybersecurity Risk Assessment		
• Comprehensive vulnerability assessment		
• Configuration review of:		
○ Network		
○ Identity systems		
○ HPC infrastructure		
○ Cloud environments		
• Risk scoring and prioritization		
• Gap analysis against recognized frameworks (e.g., NIST CSF)		
• Executive summary for leadership		
• Remediation roadmap with timelines		
• Annual emergency drills		
5. Network Security Enhancements:		

• Zero-Trust Networks Access		
○ Session-based access control		
○ Identity-centric access policies		
○ Continuous authentication during session		
○ Least-privilege access enforcement		
○ Application-level segmentation in addition to network-level VPN		
○ Replacement or modernization of traditional VPN		
• Device Posture Assessment		
○ Pre-access and continuous posture validation		
○ Verification of OS		
▪ OS version and patch level		
▪ Endpoint protection status		
▪ Disk encryption		
▪ Device compliance policies		
• Secure Remote Access via encrypted access to:		
○ HPC clusters		
○ Research applications		
○ Internal web applications		
○ Administrative systems		
• Additional Requirements		
○ Scalability to support high concurrent users		

○ Support for on-prem environments		
○ Granular logging of session activity		
6. Identity Management and MFA		
• Identity & Access Management (IAM)		
○ Integration with existing directory services (e.g., Active Directory, LDAP)		
○ Support for SSO (SAML, OIDC, OAuth)		
○ Role-based access control (RBAC)		
• Multi-Factor Authentication (MFA)		
○ Support for:		
▪ Push-based authentication		
▪ FIDO2/passwordless authentication		
○ Step-up authentication for privileged or sensitive actions		
• Identity Governance – CAIR will use IBM Concert, utilizing our internal systems for the following:		
○ Access certification campaigns		
○ Automated provisioning/deprovisioning		
○ Dormant account detection		
○ Enforcement of least privilege		
Optional requirements for optimization:		
7. Data Security Monitoring & Real-Time Audit		
• Database Activity Monitoring (DAM)		

○ Real-time monitoring of:		
▪ SQL queries		
▪ Privileged activity		
▪ Bulk exports		
▪ Data exfiltration attempts		
○ Detection of anomalous user behavior		
• Data Lake & Unstructured Data Monitoring		
○ Monitoring access to:		
▪ Object storage		
▪ Data lakes		
▪ File shares		
○ Alerting on:		
▪ Mass downloads		
▪ Suspicious access patterns		
▪ Access outside business norms		
• User Behavior Analytics (UEBA)		
○ Baseline user activity		
○ Identify risky or anomalous behavior		
○ Risk scoring of users and sessions		
• Audit & Compliance Reporting		
○ Immutable audit logs		
○ Compliance-ready reporting (e.g., ISO 27001, NIST, HIPAA if applicable)		

○ Long-term log retention options		
Interface/Integration Requirements		
Vendors must provide:		
• High-level and detailed architecture diagrams		
• Integration roadmap with existing infrastructure		
• API availability		
• Deployment model		
• Scalability benchmarks		
• Data residency controls		
Compliance and Regulatory Alignment		
Vendor must demonstrate alignment with:		
• NIST Cybersecurity Framework		
• ISO 27001		
• SOC 2		
• Treasury Board of Canada Secretariat guidance for Protected B information		
• Canadian baseline security controls (ITSG-33)		
• Applicable research or regulatory standards		
Service Level Agreements (SLAs)		
• Uptime guarantees		
• Incident response times		
• Support response times		
• Escalation processes		
• Penalties for SLA breaches		
Reporting Requirements		
• Reporting on near-real time detection and event correlation		
• Reporting, visualization and exporting capabilities provided		
• Allowing manual report creation, modification of existing reports, saving and sharing for team use		

Running manual data queries and exporting results to a structured data standard		
Usability Requirements		
Dashboard capabilities and assistance in identifying, investigating, interpreting and managing events		
Dashboard customization		
Workflow creation and automation		
Data retention; e.g. duration and cost effectiveness		

Contracting Information

- Preferred 3-year contract, plus possible extension
- Expected user base 400-800 users/year
- The vendor shall propose the most cost-efficient and effective solution that delivers all desired functionality outlined in this RFP, or an equivalent alternative that achieves the desired outcomes. Any deviations from the desired functionality must be clearly identified, along with the rationale for the proposed alternative.

Pricing Structure

Please include:

- Subscription licensing
- Per-user pricing (identify economical changes in tier pricing)
- Per-node pricing
- Log ingestion costs
- Managed services fees
- Professional services costs
- Multi-year discount options

- Data sovereignty and vendor access control
- Transition and exit strategy

Submission Requirements

- Refer to proposal requirements and content
 - Vendor Qualifications
 - Project Approach
 - Proposals
 - Contracting model and subcontractor information
- Bidders must explicitly identify any gaps between their solution and Protected B requirements and propose mitigation strategies or compensating controls – longer term roadmap.

Sanctions and Export Control

- Contractors shall represent and warrant that it will comply with all applicable Canadian and international and trade compliance regulations and related government restrictions (Sanctions and Export Control Laws) in its performance of the Contract.
- The Contractor shall ensure that no products, services, personnel, software, hardware, technical information, or third-party components provided under the Contract violate applicable sanctions, export restrictions, or trade control requirements.
- The Contractor shall promptly notify CAIR of any circumstance that may affect its ability to comply with such obligations.

Data Ownership and Sovereignty

- All security telemetry, logs, reports, alerts, forensic artifacts, configurations, incident records, and related data generated through the provision of services shall remain the sole property of CAIR and/or Memorial University.
- Vendor personnel may only access CAIR data as required for service delivery and in accordance with approved access control procedures.
- Vendor access to CAIR systems and data must be logged, monitored, and auditable. CAIR reserves the right to audit vendor access records and privileged activities associated with service delivery.
- Vendor personnel with access to CAIR systems or security data must be identified and subject to appropriate personnel screening and background verification processes consistent with Protected B alignment objectives.

- The vendor shall not use CAIR data for artificial intelligence model training, commercial product development, or any purpose unrelated to delivery of contracted services.
- The vendor shall not share, aggregate, contribute, or otherwise disclose CAIR data to external threat intelligence platforms, data lakes, or third parties without prior written approval from CAIR.
- All CAIR data must remain within approved Canadian hosting environments unless otherwise approved in writing by CAIR.
- The Contractor shall ensure that all subcontractor selection and performance comply with applicable sanctions and export control law

Contract Exit and Transition Requirements

Bidders must provide a documented exit and transition strategy that includes:

- Return of all CAIR-owned data.
- Export of logs, reports, alerts, configurations, and incident history in industry-standard formats.
- Support knowledge transfer activities & transition process.
- Secure destruction of retained CAIR data following contract termination.
- The proposal must identify
 - Data retention periods following contract termination
 - Available export formats.
 - Any transition-related costs.

APPENDIX B – SUBMISSION FORM

1. Proponent's Information

Please fill out the following form, naming one person to be the Proponent's contact for the Open Call process and for any clarifications or communication that might be necessary.	
Full Legal Name of Proponent:	
Any Other Relevant Name under which Proponent Carries on Business:	
Street Address:	
City, Province/State:	
Postal Code:	
Phone Number:	
Fax Number:	
Company Website (if any):	
Proponent's Contact Name and Title:	
Proponent's Contact Phone:	
Proponent's Contact Fax:	
Proponent's Contact Email:	

2. Offer

The Proponent has carefully examined the Open Call documents and has a clear and comprehensive knowledge of the Deliverables required under the Open Call. By submitting a Proposal, the Proponent agrees and consents to the terms, conditions and provisions of the Open Call, including the Form of Agreement, and offers to provide the Deliverables in accordance therewith at the rates set out in the pricing section.

3. Rates

The Proponent has submitted its rates in accordance with the instructions in the Open Call. The Proponent confirms that it has factored all of the provisions of Appendix A, including insurance and indemnity requirements, into its pricing assumptions and calculations. All prices must be in Canadian Dollars.

4. Addenda

The bidder is deemed to have read and accepted all addenda issued by the Owner. The onus is on bidders to make any necessary amendments to their bids based on the addenda. The bidder is required to confirm that it has received all addenda by listing the addenda numbers on the following line: **(For example, if Addendum 1 has been issued, enter 1 on the line. If there are two addenda, enter 1, 2)_**. Bidders who fail to complete this section will be deemed to have not received all posted addenda and shall be deemed **non-compliant**.

5. No Prohibited Conduct

The Proponent declares that it has not engaged in any conduct prohibited by this Open Call.

6. Disclosure of Information

The Proponent hereby agrees that any information provided in this Proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or by order of a court or tribunal. The Proponent hereby consents to the disclosure, on a confidential basis, of this Proposal by the Owner to the advisers retained by the Owner to advise or assist with the Open Call process, including with respect to the evaluation of this Proposal.

7. Proposal Irrevocable

The Proponent agrees that its proposal shall be irrevocable for a period of **90** days following the Submission Deadline.

8. Required Signatures

Failure to submit this signature section will render the Proposal NON-COMPLIANT and the Proposal will be disqualified.

Name of Proponent's Representative

Title of Proponent's Representative

Date

I have the authority to bind the Proponent.

IN SIGNING THIS PAGE AND SUBMITTING YOUR PROPOSAL, THE PROONENT ACKNOWLEDGES HAVING READ AND UNDERSTOOD AND AGREED TO THE TERMS AND CONDITIONS OF THIS DOCUMENT.

APPENDIX C – EVALUATION CRITERIA

CAIR Cybersecurity RFP — Vendor Evaluation Scoring Matrix

#	Evaluation Criterion	What It Covers	Weight	Vendor 1 (NAME)		Vendor 2		Vendor 3		Vendor 4	
				Score (1-5)	Weighted %	Score (1-5)	Weighted %	Score (1-5)	Weighted %	Score (1-5)	Weighted %
1	Ability to Meet Functional Requirements, Solution Completeness & Protected B Alignment	Technical capability, security architecture, integration capability, scalability, demonstrated alignment with Protected B control requirements, overall completeness in meeting functional requirements	25%	1	5.0%						
2	Total Cost of Ownership	Subscription/licensing, per-user & per-node pricing, I managed services fees, professional services costs, multi-year discounts, additional/after-hours charges.	20%	1	4.0%						
3	Managed Services & Operational Capability	24/7 SOC quality, Tier 1-3 support model, SLAs (detection/response/containment), escalation fit with CAIR's proposed tiers, reporting & dashboards.	30%	1	6.0%						
4	Vendor Experience, Governance & Data Sovereignty	HPC/research references, financial stability, Prime Contractor accountability model, Canadian data residency, personnel screening, subcontractor governance.	15%	1	3.0%						
5	Implementation and Execution Approach, Continuous Improvement	Implementation timeline & milestones, team resources, execution strategy, continuous improvement process	10%	1	2.0%						
TOTAL WEIGHTED SCORE			100%		20.0%		0.0%		0.0%		0.0%

Scoring scale (1–5)
1 — Does not meet requirement / major gaps, no credible mitigation
2 — Partially meets requirement / significant gaps or unproven approach
3 — Meets requirement / solid, compliant, industry-standard approach
4 — Exceeds requirement / strong differentiators, low residual risk
5 — Significantly exceeds requirement / best-in-class, clear competitive advantage

*** PRICING FORMULA***

lowest price + proponent's price × weighting = proponent's pricing points

APPENDIX D – REQUEST FOR PROPOSAL PARTICULARS

Negotiations

Memorial University reserves the right to conduct negotiations with more than one vendor simultaneously.

Submission Requirements

- **Submission Form (Appendix B)**
- **Submission – Detailing Scope and Specifications Required**

Evaluation Committee

(Proposed) Members of the Evaluation Committee are:

Operations Manager - CAIR
Solution Architect - IBM/CAIR
MUN Director of Information, Protection and Security
Associate Director - CAIR
MUN Research Security Manager
System Administrator - CAIR