

# Cybera security services for Alberta post-secondaries

## Cybera Security Nexus

The Cybera Security Nexus provides expertise and resources to publicly-funded institutions looking to assess, prioritize, and address their cybersecurity and policy gaps. Its services include:

- An industry recognized IT security assessment framework (NIST)\*
- A foundational set of digital security policies, standards, procedures, guidelines, and baselines
- Access to a CISO-level cybersecurity consulting to provide one-on-one guidance, direction, and advice

\*This assessment is available to all members, although post-secondary institutions participating in the national Cybersecurity Initiatives Program are encouraged to take part in the National Cybersecurity Assessment (see page 3 for more details)

## Member Benefits

- Organizations can gain a thorough overview of their cybersecurity operations, and pinpoint areas they are doing well, as well as areas for improvement
- Gain support for the design, build, and monitoring of an Information Security Management System and its related activities
- Receive Information Security policies, standards, procedures, guidelines, and baseline templates, including leadership and faculty/staff engagement templates

## Membership Requirements

Available to any Cybera member organization in Alberta's public sector.

## Cost

Visit [Cybera.ca/nexus](https://Cybera.ca/nexus) to view the pricing tiers, and to find out how to join.

## Virtual Firewall Service

Most organizations host their own firewall equipment, which can drain valuable staff time and resources. The Virtual Firewall Service alleviates these issues by placing a virtual firewall upstream on Cybera's network gateway.

This service is currently geared towards smaller institutions (i.e. bandwidth traffic under 1.3 Gbps), but we expect to launch an expanded version in 2025.

## Member Benefits

- Organizations do not have to buy and host their own physical firewall appliances.
- Reduce "hair-pinning" (where internet traffic through the centralized firewall doubles back on itself), saving on bandwidth.

- Access a secure, scalable environment to trial new network technologies.
- Additional advantages of an Alberta-based cloud infrastructure: local data storage, Calgary/Edmonton redundancy, and reliable failover.

## Membership Requirements

Available to any Cybera member organization that is a part of the Internet Buying Group.

## Cost

Visit [Cybera.ca/vfs](https://Cybera.ca/vfs) to view the pricing tiers, and to find out how to join.

## Other services available through Cybera

### D-Zone Anycast DNS



Cybera has partnered with the Canadian Internet Registration Authority (CIRA) to offer members free access\* to its Domain Name System (DNS) protection and performance. The D-Zone Anycast DNS is useful for larger public and education institutions in Alberta that run their own .ca domain, and are at risk of Distributed Denial-of-Service (DDoS) attacks.

### Member Benefits

- High Reliability: D-Zone eliminates the single point of failure. DNS queries are automatically routed around outages or server failures.
- High Performance: D-Zone servers are located close to major internet hubs, reducing latency and improving performance.
- Distributed Denial-of-Service mitigation: Global servers absorb the DDoS attacks.

To learn more, visit: [Cybera.ca/cira-domain-name-system-protection](https://Cybera.ca/cira-domain-name-system-protection)

*\* Cybera will provide one free D-Zone account per interested member.*

## Security Information and Event Management



Cybera has teamed up with its 12 provincial, territorial and federal partners in Canada's National Research and Education Network (NREN) to build a Security Information and Event Management (SIEM) solution. This represents an unprecedented pan-Canadian effort to coordinate network threat monitoring, and thereby strengthen the overall security of Canada's NREN infrastructure.

To learn more, visit: [Cybera.ca/SIEM](https://Cybera.ca/SIEM)

## National Cybersecurity Initiatives Program

Funded by CANARIE, the Cybersecurity Initiatives Program (CIP) provides eligible post-secondary institutions with services that provide richer threat and vulnerability data, improved processes, and broadened expertise.

Available initiatives through CIP include:

### National Cybersecurity Assessment



Provides an annual, comprehensive assessment of your organization's cybersecurity capabilities and capacities, measured against the NIST Cybersecurity Framework.

#### Member Benefits

- Identify your organization's cybersecurity maturity and placement relative to your peers, as well as common, sector-wide strengths and priorities for support.
- Identify cybersecurity gaps at the regional and national levels, and guide future cybersecurity investments by the NREN.
- Inform your organization's cybersecurity plans and investment strategies.

### CIRA DNS Firewall



A simple-to-implement and powerful tool that adds an extra layer of protection to existing network safeguards. This made-in-Canada DNS-based firewall solution is available to educational institutions.

#### Member Benefits

- Block/redirect users (and bots) from malicious domains such as those that contain malware or are engaged in phishing.
- Block malware and phishing.
- Aggregate threat data to allow/deny traffic based on new intelligence.
- Facilitate research from new intelligence to identify new threats.

### CIRA Off-Network Protection



Extend the protection of CIRA's DNS Firewall to users' devices wherever they are accessing the internet, beyond your campus network. Helps institutions support faculty and staff in hybrid and remote working and learning environments.

### Member Benefits

- Device-level reporting
- Network management
- Support for all major operating systems

### CANSSOC Threat Feed



**CanSSOC**

Aggregates and curates threat intelligence from public and private cybersecurity threat feeds into a single block/allow list that eligible post-secondary institutions can deploy directly into their existing firewall.

### Intrusion Detection System

Tracks suspicious network behaviour to find new threats as they emerge.

Organizations that participate in the Intrusion Detection System (IDS) initiative will be able to select an IDS device that suits their existing infrastructure, and receive funding to support the participation of cybersecurity staff in the national IDS collaboration.

### CUCCIO Cybersecurity Benchmarking



A service that assesses and compares post-secondary organizations' cybersecurity processes and performance to promote evidence-based best practices.

The service includes:

- Benchmarking the cybersecurity performance of Canadian research and education (R&E) organizations.
- Continuous security monitoring of participating organizations.
- Assessing the cybersecurity performance of vendors.

Want to get involved in CIP? For more information, visit: [Cybera.ca/CIP](https://cybera.ca/CIP)

---

For additional questions about any of the security services mentioned above, contact: [projects@cybera.ca](mailto:projects@cybera.ca)