

CyberAlberta

Community of Interest

Terms of Reference

Purpose

The CyberAlberta Community of Interest is intended to inform and engage Alberta stakeholders and influence matters relating to cybersecurity with the goal of strengthening the overall cybersecurity posture of the province of Alberta.

Scope of Work

- Advise and facilitate discussion on emerging cyber threats to Alberta stakeholders;
- Promote best practices in cybersecurity;
- Engage Alberta private and public sector organizations to raise cyber threat awareness, increase cybersecurity knowledge, and/or educate to strengthen the province's cybersecurity posture;
- Foster leadership and collaboration amongst Alberta stakeholders to assist in safeguarding the province's digital systems and data assets; and
- Work collaboratively with education service providers to develop new cyber talent across the province.

Membership

Cybersecurity contacts and leads for Alberta public sector organizations, Alberta not-for-profit organizations, and Alberta-based businesses can become members of the CyberAlberta Community of Interest. Vendors and Service Providers may join this Community of Interest however may be asked to temporarily leave a meeting if the chair determines that a conflict of interest may arise due to content being discussed.

Actual membership list of contacts and contacts information will be tracked by the secretariat in a separate document.

Accountabilities and Expectations

All representatives are responsible for sharing pertinent information with the Community of Interest relating to cyber threats, cyber attacks, cyber incidents, and other cybersecurity related matters.

Members are expected to participate in meetings by asking questions, sharing experiences, and sharing ideas that may assist in strengthening Alberta's cybersecurity posture.

Third Party Rule (3PR)

Any information or documentation received from another party under the “Third Party Rule” cannot be further disclosed or shared without the consent of the originating party. All information received from other parties MUST be treated in accordance with the caveats, protection or classification level assigned by the originating party and MUST be handled in accordance with the rules and procedures established by that party. Should the recipient of information not be able to provide the same level of protection required by the originator, this should be made clear to the originator before the information is collected whenever possible.

Improper handling or disclosure of information provided by other parties may result in such information no longer being shared with the group.

Roles and Responsibilities

Chair and Secretariat

1. Solicit for and set agenda and send meeting invitations
2. Manage action items
3. Document minutes (decisions and action items)
4. Lead and facilitate meetings

Core Members

1. Attend all meetings or designate alternates with the same authority
2. Present or speak to agenda items
3. Prepare information sharing items
4. Complete action items
5. Communicate and disseminate decisions

At-will Members

1. Present or speak to agenda items
2. Prepare information sharing items
3. Complete action items where assigned
4. Communicate and disseminate decisions

COI Subcommittee Governance

Due to the wide-ranging topics in this field, there will not be enough time to discuss specifics for particular topics during the main COI meetings. To address this, COI subcommittees will be formed to provide an avenue where interested members can further discuss specific topics and related challenges to develop recommendations to resolve them.

COI subcommittees may be identified and requested during the main COI meeting. Chairs and vice chairs roles for these subcommittees will be filled by COI member volunteers.

COI Subcommittee Reporting

COI subcommittees will report back to the main COI group on a regular basis to provide updates as required. If there is Protected B or C information being discussed, there may be a requirement to hold member-specific meeting. The COI chair will determine when that is required.

If there is a lot of information to be provided, alternate channels (i.e. email, website hosting) may be used to distribute the updates to the membership.

Meeting Procedures

Meetings are to be scheduled on a regular 2 month schedule unless COI membership agrees on a different schedule (i.e. monthly, quarterly).

Ad-hoc or emergency meetings may be scheduled to discuss emergent cybersecurity related topics or events. The Chair will provide as much notification as possible for these meetings to ensure participants are aware and can attend/delegate where required.

The Chair of the COI (and future sub-committees) will ensure an effective meeting by including:

- A clear, concise and focused agenda
- Background documents delivered in advance, containing relevant, timely and accessible information in a style and format that is easily consumable
- Prepared participants
- Relevant, robust and respectful dialogue
- Raising hands (virtually for online meetings) to ask a question or make a comment – the Chair or Vice-Chair will ask participants to speak up based on first hand up, first to speak
- A record of decisions and action items are completed and sent out to COI members within 3 days of meeting
- The meeting starts and finishes on time