

STRUCTURE

1) Mandate

The Settlement and Integration Service Delivery Committee (SISDC) Data Privacy and Cybersecurity working group is a table to bring together Immigration, Refugees and Citizenship Canada (IRCC) and representatives of funded settlement organizations under the Settlement and Resettlement Assistance Program. This working group is dedicated to discussing and addressing themes of data privacy and cybersecurity within the federal Settlement and Resettlement programs in the immediate to medium term (6-12 months).

Recognizing the dynamic nature of immigration and technological landscapes, the mandate of this working group remains adaptable and responsive to evolving needs. Its core focus remains on enhancing sectoral capacity to safeguard data privacy and security, improving cybersecurity practices, and ensuring the protection of client information for IRCC-funded service provider organizations (SPOs) providing settlement and resettlement services and programs.

The SISDC Data Privacy and Cybersecurity working group reports directly to the SISDC.

2) Scope

The SISDC Data Privacy and Cybersecurity working group is not a decision-making body for the overall administration of federal Settlement and Resettlement Programs or the SISDC. This working group will assume a critical role in shaping short-term, proactive strategies aimed at bolstering the capacity of SPOs to safeguard data privacy and cybersecurity. Through informed decision-making processes, the working group will strategically navigate challenges and opportunities to enhance the resilience of IRCC-funded SPOs. Additionally, the working group will collaborate closely with SISDC to ensure seamless information exchange and alignment of efforts with SIPPC and its respective working groups where decisions intersect to foster an approach to address shared concerns.

The scope of work for the SISDC Data Privacy and Cybersecurity working group can include, but is not limited to issues of:

- Conducting an Environmental Scan on existing or past initiatives to create strategies and protocols to safeguard information
- Data management and security, confidentiality and information sharing
- Data privacy and cybersecurity innovation and capacity building

3) Objectives

The specific objectives of the SISDC Data Privacy and Cybersecurity working group are to:

- Evaluate existing sector organizations' data privacy and cybersecurity practices, trends, issues and risks to support the mapping of procedures and best practices.
- Develop comprehensive advice and protocols for safeguarding information and bolstering security measures.
- Formulate tools and resources, such as; security and confidentiality compliance frameworks, roadmap(s), checklists and fact sheets to fortify the Sector against data breaches and maintain cybersecurity.
- Liaise with the SIPPC Technology working group to define criteria for enhancing digital literacy capacity and crafting digital learning strategies and training opportunities.

All working group objectives will be formulated and finalized in alignment with the scope mentioned above, in addition to IRCC Grant and Contribution Agreement requirements and directions.

ROLES

4) Structure and Membership Rationale

Tenure

The SISDC Data Privacy and Cybersecurity working group will be co-chaired by one representative from IRCC and by one representative of SISDC, as determined by SISDC co-chairs.

The term of the Sector working group co-chair and working group is limited to three (3) years, aligned with the tenure of SISDC, or until the group completes its work, whichever is earlier.

The National Sector Engagement (NSE) Secretariat will lead the call-out and confirmation of membership for the working group using an intersectional approach to ensure equity, diversity and inclusion at the individual and organizational levels. In the event that the mandate of the working group extends beyond the three year timeline, the working group co-chairs will propose an approach to SISDC including an overview of work yet to be completed.

Membership

Membership will include, but may not be limited to, representation from Directors of IT or Business Technology from IRCC funded (re) settlement organizations, IT experts from IRCC-funded SPOs and other subject matter experts as identified by SISDC co-chairs or working group co-chairs, as well as an IRCC official from Settlement Network. In addition, membership of the SISDC Data Privacy and Cybersecurity working group will include Francophone representation to ensure the perspectives and needs of Francophone funded organizations and the clients they serve are reflected in deliberations. Membership will comprise up to eight (8) nominated representatives, including two (2) co-chairs. The size may be increased depending on the

working group's objectives, subject to SISDC co-chairs' approval. Each member will specify one alternate to cover absences.

Members are expected to represent the views of a constituency of organizations, including from small organizations and communities. Consideration will be given to ensuring working group membership reflects the specific needs, interests and experiences of diverse Sector members and stakeholders, while also ensuring participation from partners with relevant subject matter expertise (i.e. IT experts).

5) Co-Chair and Member Roles and Responsibilities

Responsibilities of Co-Chairs

In collaboration with SISDC co-chairs, working group co-chairs are responsible for:

- i) finalizing a work plan with immediate to short-term strategic objectives that align with priorities of the SISDC. The working group may ensure broad engagement and input from service providers of varying sizes, regions, capacities, etc. in relation to finalizing its draft reports/deliverables;
- ii) leading in the implementation and tracking of progress according to work plan milestones;
- iii) setting and following the agenda for working group meetings in alignment with the work plan;
- iv) ensuring the interests and experiences of various and diverse populations are considered in deliberations, including, for example, women, racialized persons, persons with disabilities, Indigenous people, linguistic minorities, sexual orientation and gender diverse groups including 2SLGBTQI+, remote, rural and northern communities;
- v) providing working group updates, in writing, on the implementation of the work plan at quarterly SISDC meetings; and
- vi) After the inaugural year of establishing the working group, co-chairs will submit a report on the group's findings and recommendations to the SISDC. Reporting frequency will be established in the work plan.

Member Responsibilities

Working group members will fairly represent the diverse voices of government and non-government settlement and integration colleagues.

Working group members will demonstrate a commitment to the success of the group by consistently attending meetings, participating in discussions, providing meaningful contributions to support the deliverables laid out in the work plan, submitting deliverables to the working group as outlined in the work plan and assigned by co-chairs, and working collegially. If a member is unable to fulfil their responsibility, the SISDC co-chairs may ask them to step down from the working group. When a position becomes vacant, a call for participation will be advertised.

PROCESS

6) Meetings

Meeting Frequency

Working Group co-chairs will decide the appropriate meeting schedule in alignment with the work plan and deliverables, in consultation with working group members. Meetings will be held virtually.

Budget

Subject to Departmental approvals and in accordance with the Treasury Board (TB) guidelines, IRCC will fund logistical support (including securing a location, hospitality and interpretation service costs if needed for meetings) for SISDC working groups. SISDC co-chairs to determine if an annual in-person working group meeting is deemed necessary.

IRCC currently funds the NSE Secretariat through Affiliation of Multicultural Societies and Serving Agencies of BC (AMSSA) to coordinate and support the sector to fully participate in the SISDC and its working groups, including canvassing members on their views and other sector-based analyses of issues, to coordinate the costs associated with in-person Sector participation (including travel, accommodation and incidental costs), and to liaise and coordinate with the SIFA Secretariat.

National Sector Engagement (NSE) Secretariat

The secretariat and coordination function to the SISDC working groups will be provided by the NSE Secretariat. The NSE Secretariat will convene SISDC Data Privacy and Cybersecurity working group meetings and provide organizational, analytical and technical support to the co-chairs of this working group. The NSE Secretariat will make arrangements for interpretation services, as required. In accordance with TB guidelines, the NSE Secretariat will coordinate the meeting location/hospitality, if working group co-chairs or members are asked to attend an annual in-person meeting.

In support of SISDC co-chairs, the NSE Secretariat will organize and disseminate all SISDC Data Privacy and Cybersecurity working group meeting agendas, documents, minutes and other relevant materials to meeting participants, SISDC and SIFA Secretariat in a timely manner. To ensure alignment between technology-focused working groups, the NSE Secretariat will share working group meeting agendas, documents, minutes and other relevant materials from the SISDC Data Privacy & Cybersecurity working group with the SIPPC Technology working group.

Settlement, Integration and Francophone Affairs (SIFA) Secretariat Function

The monitoring and tracking function to the SISDC working groups will be provided by Settlement and Integration Policy Branch, IRCC. The SIFA Secretariat will track work plans, outputs and outcomes, identify opportunities for alignment between working groups, and flag challenges and risks. Secretariat functions are provided in Annex A of the SISDC terms of reference.

Renewal of Terms of Reference

At the end of the working group's mandate, and as determined in the workplan, the SIFA Secretariat will review the Terms of Reference for the SISDC Data Privacy and Cybersecurity working group, in consultation with SISDC, and adopt any changes at that time.

OFFICIAL LANGUAGES

Agendas, key documents and other material will be made available in both official languages (OL). The working group is expected to support conducting in-person and virtual meetings in both official languages.

CONFLICT OF INTEREST

Members are committed to ensure that discussions about program and operational priorities do not provide an advantage with respect to funding any SISDC working group member, as per the "Conflict of Interest Guidelines" document presented in Annex B of the SISDC Terms of Reference.

DATE OF ADOPTION

July 18, 2024.