



IEEE Canada



IEEE Canada Public Policy Committee

Digital Sovereignty Strategy

An IEEE Canada Public Policy Committee Position Statement

Adopted June 17, 2026

The English version is authoritative. A French version follows.

La version anglaise fait foi. La version française est à la suite de la version anglaise.

Preamble:

In a world driven by advanced technologies such as artificial intelligence (AI), cloud computing, and cybersecurity frameworks, Canada must assert sovereignty over its digital and technological ecosystem to secure its national interests. Digital sovereignty in technology ensures Canadian's control over critical systems, data, and innovation, safeguarding against external influence and systemic vulnerabilities [1].

Acknowledging the policies recently developed by the Treasury Board of Canada related to the Government of Canada (GC) infrastructure and services [2], the IEEE Canada Public Policy Committee reinforces the critical importance of digital sovereignty in empowering innovation and ensuring ethical governance of emerging technologies, outlining a technology-driven strategy rooted in technical excellence, global collaboration, skilled workforce development and public trust to guide Canada's secure, innovative and independent digital future. Digital sovereignty should not be interpreted as technological isolation or closed technological ecosystems.



IEEE Canada



IEEE Canada Public Policy Committee

Recommendations:

IEEE Canada recommends the following policies:

- 1) **Develop Sovereign and Resilient Digital Infrastructure:** Strengthen domestic cloud and high-performance computing infrastructure for AI and data analytics with state-of-the-art cyber security protection. In collaboration with service providers, ensure national coverage of resilient fiber infrastructure with government oversight to avoid bottlenecks, single points of failure, and unnecessary cross border routing of Canadian user traffic. Establish energy-efficient “sovereign data centers” in cold climate regions such as northern Canada, involving indigenous communities where relevant. Leverage potential industrial policy tools – such as strategic procurement, tax incentives, public-private partnerships, and de-risking mechanisms – that could support a more sovereign and resilient tech supply chain. Recognize data centers as critical infrastructure, ensuring robust physical and cybersecurity protections.
- 2) **Advance Data Governance:** Mandate data localization in Canada for AI training datasets and sensitive government systems, with explicit compliance obligations for foreign tech providers. Require that AI models used on sensitive Canadian data incorporate representative training data, transparency, accountability, bias evaluation mechanisms, and appropriate governance processes to help reduce harmful bias and improve trustworthiness. Promote strong data governance frameworks that protect the rights, privacy, and interests of all Canadians while recognising the distinct rights of Indigenous communities to govern data related to their peoples, lands, and cultural heritage. [3]
- 3) **Drive Canadian Technology Innovation:** Support Canadian startups in AI, quantum computing, cloud architectures, and cybersecurity, with emphasis on open-source software, standards, hardware development, and semiconductor innovation [4], with an aim at Canadian deployment. Strengthen partnerships between Canadian universities, technology firms or startups, and government to accelerate breakthroughs in secure, algorithms and systems. Reinforce established manufacturing and innovation clusters (e.g., advanced manufacturing corridors, AI hubs) as natural anchors for sovereign digital infrastructure and secure hardware production. Ensure



IEEE Canada



IEEE Canada Public Policy Committee

Indigenous representation to integrate traditional knowledge. Improve access to critical compute resources in Canada, particularly by lowering barriers to compute for early-career researchers, non-profits, and public-interest projects.

- 4) **Build a Skilled Technical Workforce:** Reform of the education system by investing in updating national curricula that integrate technology skills - such as ethical AI [5], coding, data analytics, cybersecurity, and digital fluency - from early education through higher levels. Introduce critical cyber security training to employees of the public sector, emphasizing sovereignty risks such as supply chain vulnerabilities, unauthorized access, or dependency. Include dedicated modules on safeguarding Indigenous cultural data. Enhance public awareness and confidence in AI, to help understand and avoid biases, through comprehensive digital literacy initiatives for all age groups, delivered via strategic partnerships between government, academia, and non-profits, to ensure availability of trusted, technically excellent, and interoperable solutions, including domestic focus where strategically important, and secure Canada's AI sovereignty.
- 5) **Lead Global Technology Standards and International Alliances:** Lead development of global, consensus-based sovereignty-focused standards for AI and cloud computing, promoting that Canadian values help shape global technology governance. Strengthen sovereignty tools and processes through bilateral partnerships with allies and multilateral bodies such as the G7, emphasizing supply chain security.

Call to Action:

IEEE Canada urges Canadian policymakers to strengthen a comprehensive Digital Sovereignty Strategy that integrates: resilient digital infrastructure, sovereign data management, technical standards, ethical governance, skilled workforce development, and inclusive innovation. By doing so, Canada can secure its digital future while contributing meaningfully to global technological progress.



IEEE Canada



IEEE Canada Public Policy Committee

Background:

In recent years, digital sovereignty has become a growing concern for policymakers, who argue that excessive control is concentrated in a few entities, the tech market lacks sufficient competition, and a handful of tech giants wield disproportionate power by amassing vast amounts of user data and consuming natural resources at an unprecedented pace. A recent study by the World Economic Forum [6] describes the different approaches that countries follow in addressing the various aspects of digital sovereignty including cyber sovereignty, technological sovereignty and data sovereignty, which collectively refer to the ability of a country to have control over its digital destiny – the data, hardware and software that citizens rely on and create.

The European University Institute [7] explains that digital sovereignty broadly emphasizes increased state authority over the digital realm, encompassing the physical layer (infrastructure and hardware), the code layer (standards, rules, and design), and the information layer (content and personal data). Its objectives include bolstering resilience through local production of critical hardware like semiconductors, enhancing cybersecurity through stronger network security regulations, and curbing the influence of foreign state-owned enterprises by implementing stricter oversight of Foreign Direct Investments (FDIs).

The Government of Canada has published a policy statement addressing digital sovereignty in the Government of Canada (GC) infrastructure and services, titled: “Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada” [2]. The statement highlights challenges related to jurisdictional complexity, reliance on global suppliers, evolving cyber security risks, and internal capacity, which influence the ability of GC to maintain digital sovereignty. It calls for strengthening contractual and policy mechanisms, improving supply assurance, and enhancing technical safeguards, to maintain the security and reliability of government information and systems. A recent example of a “sovereign data centers” is the deployment of a 90MW hyperscale data center in Alberta [8].

Disclaimer:

This statement was developed by IEEE Region 7 (Canada) and represents the considered judgment of a group of IEEE members with expertise in the subject field. The positions taken by IEEE Region 7 (Canada) do not necessarily reflect the views of IEEE or its other Organizational Units.



IEEE Canada



IEEE Canada Public Policy Committee

References:

- [1] “How Canada could achieve digital sovereignty,” *Policy Options*, May 2025. [Online]. <https://policyoptions.irpp.org/2025/05/digital-sovereignty-canada/>
- [2] “Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada” Nov. 2025 [Online]. <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html>
- [3] Canadian Data Governance Standardization Roadmap, *Standards Council of Canada*, May 2024. [Online]. https://scc-ccn.ca/system/files/2024-05/scc_data_gov_roadmap_en.pdf
- [4] Information and Communications Technology Council (ICTC), A National Semiconductor Strategy for Canada: Policy Options and Recommendations, ICTC-CTIC, Ottawa, ON, Canada, Nov. 2025. [Online]. <https://ictc-ctic.ca/reports/a-national-semiconductor-strategy-for-canada>
- [5] IEEE 7000™ series standards (addresses ethical and societal considerations in AI and autonomous systems, including transparency, privacy, algorithmic bias, and accountability). *IEEE 7000-2021* [Online]. <https://standards.ieee.org/ieee/7000/6781/>
- [6] “What is digital sovereignty and how are countries approaching it?,” *World Economic Forum*, Jan. 2025. [Online].: <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>
- [7] “Digital sovereignty in a post-globalised world,” *European University Institute*, Jun. 2025. [Online]. <https://www.eui.eu/events?id=577256>
- [8] “Alberta announces AI Data Centres Strategy: A \$100-billion vision for the future,” *MLT Aikins*, Dec. 2024. [Online]. <https://www.mltaikins.com/insights/alberta-announces-ai-data-centres-strategy-a-100-billion-vision-for-the-future/>

Contact information:

Should you want to get in touch with the IEEE Canadian Public Policy Committee or find out more about its activities, please go to <https://ieeecanada.org>



IEEE Canada



IEEE Canada Public Policy Committee

About IEEE Canada:

IEEE Canada is the Canadian arm (also known as Region 7) of the Institute of Electrical and Electronics Engineers (IEEE) as well as the constituent society of the Engineering Institute of Canada (EIC) for the technical fields of electrical, electronics, and computer engineering. It operates 21 sections (local organizations) arranged in 3 areas (Western, Central, and Eastern Canada), as well as over 50 student branches in universities and colleges. It provides resources to assist students and members in upgrading their knowledge base and professional skills. It also organizes two annual Region 7 conferences (CCECE and EPEC) and one bi-annual conference (ANTEM) in Canada and one global conference (IHTC) in Canada every three years.



IEEE Canada



IEEE Canada Public Policy Committee

Stratégie de souveraineté numérique

Déclaration de position du Comité de politique publique de l'IEEE Canada

Adopté le 17 juin 2026

La version anglaise, qui précède fait foi.

Préambule :

Dans un monde marqué par l'essor de technologies avancées telles que l'intelligence artificielle (IA), l'informatique en nuage et les cadres de cybersécurité, le Canada doit affirmer sa souveraineté sur son écosystème numérique et technologique afin de protéger ses intérêts nationaux. La souveraineté numérique technologique assure aux Canadiens le contrôle des systèmes critiques, des données et de l'innovation, tout en protégeant des influences étrangères et les vulnérabilités systémiques [1].

Prenant acte des politiques récemment élaborées par le Conseil du Trésor du Canada concernant l'infrastructure et les services du gouvernement du Canada [2], le Comité de politique publique (CPP) de l'IEEE Canada souligne l'importance cruciale de la souveraineté numérique pour stimuler l'innovation et garantir une gouvernance éthique des technologies émergentes. Le CPP propose une stratégie axée sur la technologie, fondée sur l'excellence technique, la collaboration mondiale, le développement d'une main-d'œuvre qualifiée et la confiance du public, afin de guider l'avenir numérique du Canada vers un modèle plus sûr, innovant et indépendant. La souveraineté numérique ne doit pas être interprétée comme un isolement technologique ou des écosystèmes technologiques fermés.

Recommandations :



IEEE Canada



IEEE Canada Public Policy Committee

IEEE Canada recommande les politiques suivantes :

- 1) **Développer une infrastructure numérique souveraine et résiliente** : Renforcer les infrastructures nationales d'informatique en nuage et de calcul haute performance pour l'IA et l'analyse des données, en les dotant de protection de cybersécurité de pointe. En collaboration avec les fournisseurs de services, assurer une couverture nationale d'infrastructure de fibre optique résiliente sous supervision gouvernementale afin d'éviter les goulots d'étranglement, les points de défaillance uniques et l'acheminement transfrontalier inutile du trafic des utilisateurs canadiens. Établir des « centres de données souverains » écoénergétiques dans des régions au climat froid, comme le nord du Canada, en impliquant les communautés autochtones le cas échéant. Mettre à profit des leviers de politique industrielle, tels que l'approvisionnement stratégique, les incitatifs fiscaux, les partenariats public-privé et les mécanismes d'atténuation des risques, afin de soutenir une chaîne d'approvisionnement technologique plus souveraine et résiliente. Reconnaître les centres de données comme infrastructure critique, en garantissant des protections physiques et de cybersécurité robuste.
- 2) **Renforcer la gouvernance des données** : Imposer la localisation, au Canada, des données d'entraînement de l'IA et des systèmes gouvernementaux sensibles, assortie d'obligations de conformité strictes et explicites pour les fournisseurs de technologies étrangers. Exiger que les modèles d'IA exploitant des données sensibles canadiennes intègrent des jeux d'entraînement représentatifs, fassent preuve de transparence et d'imputabilité, incluent des mécanismes d'évaluation des biais et reposent sur des processus de gouvernance appropriés afin d'atténuer les biais préjudiciables et d'accroître la fiabilité. Promouvoir des cadres de gouvernance des données robustes qui protègent les droits, la vie privée et les intérêts de l'ensemble des Canadiens tout en reconnaissant les droits distincts des communautés autochtones quant à la gouvernance de leur données, de leurs terres et de leur patrimoine culturel.[3]
- 3) **Stimuler l'innovation technologique canadienne** : Soutenir les entreprises en démarrage canadiennes dans les domaines de l'IA, de l'informatique quantique, des architectures infonuagiques et de la cybersécurité, en mettant l'accent sur les



IEEE Canada Public Policy Committee

logiciels libres, les normes, le développement de matériel et l'innovation dans le domaine des semi-conducteurs [4] tout en visant un déploiement au Canada. Renforcer les partenariats entre les universités canadiennes, les entreprises technologiques ou en démarrant le gouvernement afin d'accélérer les percées en matière d'algorithmes et de systèmes sécurisés. Consolider les pôles manufacturiers et d'innovation existants (par exemple, les corridors de fabrication de pointe et les pôles d'IA) en tant que piliers d'une infrastructure numérique souveraine et de la production de matériel sécurisé. Garantir une représentation adéquate des peuples autochtones afin d'intégrer leurs savoirs traditionnels. Améliorer l'accès aux ressources de calcul critiques au Canada, notamment en levant les obstacles à l'accès aux capacités de calcul pour les chercheurs en début de carrière, les organismes à but non lucratif et les projets d'intérêt public.

- 4) **Former une main-d'œuvre technique qualifiée :** Moderniser le système éducatif en investissant dans la mise à jour des programmes d'études nationaux afin d'y intégrer des compétences technologiques – telles que l'éthique de l'IA [5], la programmation, l'analyse de données, la cybersécurité et la maîtrise du numérique – de l'enseignement primaire jusqu'aux études supérieures. Mettre en place des formations ciblées en cybersécurité pour les employés du secteur public, en mettant l'accent sur les enjeux de souveraineté tels que la vulnérabilité des chaînes d'approvisionnement, les accès non autorisés ou la dépendance technologique. Intégrer des modules consacrés à la protection des données culturelles autochtones. Accroître la sensibilisation et la confiance du public envers l'IA par le déploiement d'initiatives globales de littératie numérique pour tous les groupes d'âge. Ces initiatives, menées grâce à des partenariats stratégiques entre le gouvernement, le milieu universitaire et les organismes à but non lucratif viseront à favoriser la compréhension des enjeux et à prévenir les biais. L'objectif est de garantir la disponibilité de solutions fiables, performantes et interopérables, tout en privilégiant des solutions d'origine nationale lorsque cela est stratégiquement nécessaire, afin d'assurer la souveraineté du Canada en matière d'IA.

- 5) **Diriger l'élaboration de normes technologiques mondiales et les alliances internationales :** Prendre l'initiative de l'élaboration, par le consensus, de normes



IEEE Canada



IEEE Canada Public Policy Committee

technologiques mondiales, qui favorisent la souveraineté numérique en matière d'IA et d'informatique en nuage, tout en veillant à ce que les valeurs canadiennes contribuent à façonner la gouvernance mondiale du développement des technologies. Renforcer les mécanismes et les capacités en matière de souveraineté par l'entremise de partenariats bilatéraux avec des pays alliés et des instances multilatérales tels que le G7, en accordant une attention particulière à la sécurité des chaînes d'approvisionnement.

Appel à l'action :

IEEE Canada exhorte les décideurs publics canadiens à adopter et à renforcer une stratégie nationale de souveraineté numérique reposant sur : une infrastructure numérique résiliente, une gestion souveraine des données, des normes techniques, une gouvernance responsable et éthique, le développement d'une main-d'œuvre hautement qualifiée ainsi qu'un écosystème d'innovation inclusif et compétitif. En mettant en œuvre une telle stratégie, le Canada sera mieux positionné pour renforcer sa résilience numérique et sa souveraineté numérique, tout en contribuant de manière significative aux progrès technologiques mondiaux.

Contexte :

Au cours des dernières années, la souveraineté numérique s'est imposée comme un enjeu stratégique pour les gouvernements. Les décideurs publics s'inquiètent de la concentration du pouvoir entre les mains d'un nombre restreint d'entreprises technologiques, d'un manque de concurrence au sein des marchés numériques et de l'influence grandissante de quelques acteurs mondiaux qui contrôlent d'importants volumes de données utilisateurs, tout en exerçant une pression croissante et sans précédent sur les ressources naturelles nécessaires au développement des infrastructures numériques. Une étude récente du Forum économique mondial [6] met en lumière les différentes approches adoptées par les Etats pour renforcer leur souveraineté numérique, notamment en matière de cyber souveraineté, de souveraineté technologique



IEEE Canada



IEEE Canada Public Policy Committee

et de souveraineté des données. Ensemble, ces dimensions renvoient à la capacité d'un pays à exercer un contrôle sur son avenir numérique, notamment en ce qui concerne les données, les infrastructures, les équipements, les logiciels et les plateformes numériques sur lesquels les citoyens comptent et qu'ils créent.

L'Institut universitaire européen [7] définit la souveraineté numérique comme le renforcement de la capacité des États à exercer leur autorité sur l'ensemble de l'écosystème numérique. Cette approche couvre les infrastructures physiques (), les technologies et les normes qui régissent les systèmes numériques ainsi que les données et les contenus numériques. Elle vise notamment à accroître la résilience des chaînes d'approvisionnement par le développement de capacités nationales de production locale de technologies stratégiques telles que les semi-conducteurs, à renforcer la cybersécurité au moyen de cadres réglementaires plus rigoureux sur la sécurité des réseaux et à réduire l'influence des entreprises étatiques étrangères en appliquant une surveillance accrue des investissements directs étrangers (IDE).

Le gouvernement fédéral du Canada a publié le cadre de politique « Souveraineté numérique : Un cadre pour améliorer la préparation numérique du gouvernement du Canada » [2] qui établit les principes directeurs visant à renforcer la souveraineté numérique de l'administration fédérale. Le document souligne plusieurs défis, notamment la complexité des cadres juridiques et réglementaires, la dépendance à l'égard de fournisseurs mondiaux de technologies, l'évolution constante et rapide des menaces en cybersécurité et la nécessité de développer des capacités internes à l'état, qui affectent la capacité du Gouvernement Canadien à préserver sa souveraineté numérique. Il préconise le renforcement des mécanismes contractuels et de gouvernance, une plus grande résilience des chaînes d'approvisionnement ainsi que des mesures techniques accrues afin d'assurer la sécurité, l'intégrité, et la disponibilité des données et des systèmes gouvernementaux. Le déploiement d'un centre de données hyperscale de 90 MW en Alberta [8] est un exemple récent de « centre de données souverains ».



IEEE Canada



IEEE Canada Public Policy Committee

Avertissement :

Cette déclaration a été élaborée par la Région 7 de l'IEEE (Canada) et représente l'avis éclairé d'un groupe de membres de l'IEEE possédant une expertise dans le domaine. Les positions prises par la Région 7 de l'IEEE (Canada) ne reflètent pas nécessairement celles de l'IEEE ni de ses autres instances.

References:

- [1] "How Canada could achieve digital sovereignty," *Policy Options*, May 2025. [Disponible en ligne]. <https://policyoptions.irpp.org/2025/05/digital-sovereignty-canada/>
- [2] Souveraineté numérique : Un cadre pour améliorer la préparation numérique du gouvernement du Canada» Octobre 2025 [Disponible en ligne]
<https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuance/souverainete-numerique/souverainete-numerique-cadre-ameliorer-preparation-numerique.html>
- [3] La feuille de route du Collectif canadien de normalisation, May 2024. [Disponible en ligne]. https://scc-ccn.ca/system/files/2024-05/scc_data_gov_roadmap_en.pdf
- [4] "Digital sovereignty in a post-globalised world," *European University Institute*, Jun. 2025. [Disponible en ligne]. <https://www.eui.eu/events?id=577256>
- [5] IEEE 7000™ series standards (aborde les considérations éthiques et sociétales liées à l'IA et aux systèmes autonomes, notamment la transparence, la confidentialité, les biais algorithmiques et la responsabilité). [IEEE 7000-2021](https://standards.ieee.org/ieee/7000/6781/) [Disponible en ligne].
<https://standards.ieee.org/ieee/7000/6781/>
- [6] "What is digital sovereignty and how are countries approaching it?," *World Economic Forum*, Jan. 2025. [Disponible en ligne].
<https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>
- [7] "Digital sovereignty in a post-globalised world," *European University Institute*, Jun. 2025. [Disponible en ligne]. <https://www.eui.eu/events?id=577256>
- [8] "Alberta announces AI Data Centres Strategy: A \$100-billion vision for the future," *MLT Aikins*, Dec. 2024. [Disponible en ligne]. <https://www.mltaikins.com/insights/alberta-announces-ai-data-centres-strategy-a-100-billion-vision-for-the-future/>



IEEE Canada



IEEE Canada Public Policy Committee

Coordonnées :

Si vous souhaitez contacter le Comité de politique publique d'IEEE Canada ou en savoir plus sur ses activités, veuillez consulter : <https://ieeecanada.org>

À propos d'IEEE Canada :

IEEE Canada est la division canadienne (également connue sous le nom de la Région 7) de l'institut des ingénieurs électriciens et électroniciens (IEEE) aussi bien que la société constitutive de l'institut canadien des ingénieurs (ICI) pour les champs techniques de l'électricité, de l'électronique, et de l'ingénierie informatique.

Elle regroupe **21 sections** (organisations locales) réparties en **3 zones** (Ouest, Centre et Est du Canada), ainsi que plus de **50 branches étudiantes** dans des universités et collèges. IEEE Canada fournit des ressources pour aider les étudiants et les membres à améliorer leurs connaissances et leurs compétences professionnelles.

Elle organise également deux conférences régionales annuelles (de la région 7) : CCECE et EPEC, une conférence biennale : ANTEM et une conférence mondiale : IHTC (au Canada tous les trois ans).