OECD AI Transparency Report

Organization: TELUS (CA) **Reporting Period:** Q2 2025 **Published:** April 11, 2025

Section 1 – Risk identification and evaluation

a. How does your organization define and/or classify different types of risks related to AI, such as unreasonable risks?

TELUS' approach to AI risk management is focused on data governance, responsible AI practices, trust-building, and ethical considerations. TELUS has established an AI Policy for responsible governance and use of AI across the organization. This Policy requires that initiatives involving AI Systems use our Data Enablement Plan process to identify and review risk. TELUS views AI risks as multifaceted issues that require oversight at the executive level, policy development, and the establishment of best practices for responsible and ethical use of AI technologies.

TELUS has defined a Data Risk Management Policy and Framework used across the lifecycle of advanced AI systems to align stakeholders and support risk classification. The policy defines how TELUS identifies, assesses, treats and monitors risks relating to the use and management of data. The assessment and classification of risk under this Policy and Framework determine the level at which decisions around risk, including acceptance, are made, in alignment with the requirements for use, development and deployment of AI in our AI Policy.

TELUS is committed to using AI in a way that will extend our capabilities to give back to the broader community and contribute to a friendlier future. We believe that human passion to innovate, coupled with strong ethical AI design principles, can create a powerful and positive transformation of our society. TELUS uses, develops, deploys, procures and provisions AI Systems in accordance with our Data Principles (see https://www.telus.com/Trust), our legal obligations and our Code of Ethics and Conduct (see https://www.telus.com/en/about/policies-and-disclosures/code-of-ethics-and-conduct). For example, TELUS will not use AI to deploy subliminal or purposefully manipulative techniques that distort individuals' abilities to make informed decisions, or exploit vulnerabilities of individuals or groups based on age, disability, or social/economic status in ways that could cause harm.

b. What practices does your organization use to identify and evaluate risks such as vulnerabilities, incidents, emerging risks and misuse, throughout the AI lifecycle?

TELUS has established an AI Policy for responsible governance and use of AI across the organization. It affirms TELUS' dedication to developing, using and deploying AI technologies in

a way that drives positive change, while managing risks and ensuring appropriate safeguards are in place. The AI Policy requires that AI systems are used, developed, deployed, procured and provisioned in accordance with our Data Principles (see https://www.telus.com/Trust), our legal obligations and our Code of Ethics and Conduct (see https://www.telus.com/en/about/policies-and-disclosures/code-of-ethics-and-conduct).

A key method for identification of risks across the AI lifecycle is through our Data Enablement Plan. The plan unifies our risk assessment processes for Responsible AI, Privacy Impact Assessment and Secure by Design, including cybersecurity, into a single touchpoint and improves our agility through in-business data stewardship.

Data Stewards are team members appointed by their business unit for their in-depth knowledge of their team's data uses and the intended strategy for data. To prepare them to support in the process, they participate in a certification training program, which equips and empowers them to understand responsible use of AI through data privacy, security and governance. Across the AI lifecycle, business and technology teams are active participants in the identification of risk with the support of TELUS' data governance processes.

AI models and systems are validated and verified before moving beyond the development stage with enhanced assessment and testing requirements identified through the enterprise Data Enablement Plan process. This provides consistency, reliability and alignment with TELUS' commitment to Responsible AI. TELUS uses MLOps and LLMOps practices for ongoing governance of AI throughout the lifecycle.

c. Describe how your organization conducts testing (e.g., red-teaming) to evaluate the model's/system's fitness for moving beyond the development stage?

AI models and systems are validated and verified before moving beyond the development stage with enhanced assessment and testing requirements identified through the enterprise Data Enablement Plan process. This provides consistency, reliability and alignment with TELUS' commitment to Responsible AI.

As identified through our Data Enablement Plan, TELUS may use its cross-functional purple teaming approach for evaluation of an AI system. This is a collaborative method where team members and experts from different teams, background and knowledge of AI work to identify weaknesses, vulnerabilities, and gaps in generative AI systems through adversarial testing and address them with relevant mitigations. See: https://www.fuelix.ai/post/how-to-bake-responsible-ai-into-generative-ai-deployments---go-purple

A report is compiled on the testing methodology, major findings, recommendations, and any remaining unmitigated issues or risks in order to address them with the team before implementation of the solution.

d. Does your organization use incident reports, including reports shared by other organizations, to help identify risks?

Yes

e. Are quantitative and/or qualitative risk evaluation metrics used and if yes, with what caveats? Does your organization make vulnerability and incident reporting mechanisms accessible to a diverse set of stakeholders? Does your organization have incentive programs for the responsible disclosure of risks, incidents and vulnerabilities?

Our risk identification and evaluation methodologies include both quantitative techniques (e.g. query acceptance rate, rejection rate) and qualitative assessments to assess the potential impacts of a given risk or vulnerability and understand the contexts in which they occur. For example, when using generative AI systems, risks and vulnerabilities are assessed using a purple team approach.

The TELUS Purple Teaming approach is a collaborative method designed to identify weaknesses, vulnerabilities, and gaps in generative AI systems through adversarial testing and address them with relevant mitigations. In addition to the participation from the Software Developers, Data Scientists and AI Engineers, it emphasizes the participation of diverse individuals with varying expertise and technical literacy to gain comprehensive insights into the system's shortcomings and how real users may interact with the solution.

Reporting of AI incidents are required by our AI policy, and reporting is accessible to any customer or individual through our support lines. Our AI systems are developed with feedback mechanisms for users to report incidents or vulnerabilities.

f. Is external independent expertise leveraged for the identification, assessment, and evaluation of risks and if yes, how? Does your organization have mechanisms to receive reports of risks, incidents or vulnerabilities by third parties?

Using a risk-based approach, use cases are submitted for independent external tests and reviews. We work with third parties who have independent expertise and automated tooling to support this type of testing.

External parties can contact our support lines to report risks, incidents or vulnerabilities.

g. Does your organization contribute to the development of and/or use international technical standards or best practices for the identification, assessment, and evaluation of risks?

TELUS participates in forums to develop, advance and adopt shared standards for ensuring the trustworthiness of AI, including the Standards Council of Canada National AI & Data Governance Standards Collaborative, NIST AI Safety Consortium, Responsible AI Institute, IAPP AI Governance Global (Foundational Supporter), MILA - Quebec Artificial Intelligence Institute and Vector Institute.

h. How does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks, in particular systemic risks?

We believe responsible use of AI requires input from a diverse set of voices. With a human-centred approach, we can build trust in our digital world and make a friendly future for all. We have engaged with academic and research institutions to help drive out this research. Our annual TELUS AI Report shared the views from thousands of people about their thoughts on AI - their concerns, hopes and opinions about where this powerful technology should be headed. The report is made available publicly at: www.telus.com/ResponsibleAI

TELUS is proud to have been among the first (and the first telecom) in Canada to sign the Government of Canada's voluntary code of conduct for generative AI (GenAI), which seeks transparent, equitable and responsible development of GenAI technology. https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems.

Any further comments and for implementation documentation

No answer provided

Section 2 – Risk management and information security

a. What steps does your organization take to address risks and vulnerabilities across the AI lifecycle?

TELUS favors a cross-functional purple teaming approach to understand potential vulnerabilities with generative AI systems, where team members and experts from different teams, background and knowledge of AI participate in adversarial testing and the discussion regarding the mitigation strategy. See: https://www.fuelix.ai/post/how-to-bake-responsible-ai-into-generative-ai-deployments---go-purple

Where purple teaming is determined to be appropriate, TELUS' approach is structured into the following steps, each with specific deliverables:

1.Expected AI behaviours are defined and potential risks and negative repercussions from misuse, damage, and abuse are identified.
2.Test scenarios to evaluate identified risks are defined, using various techniques.
3.Test cases are executed and results are assessed. Outputs are annotated and measured.
4.Test cases are continually refined to further identify opportunities for improved guardrails and protection layers.
5.Results are reported to developers for mitigation, with retesting after implementation until satisfactory outcomes are achieved.

b. How do testing measures inform actions to address identified risks?

TELUS follows its Data Risk Management Policy and Framework which moves the team from the risk identification step to the risk treatment step. Vulnerabilities and risks identified by internal or external stakeholders testing exercises are addressed by implementing mitigation techniques and strategies, followed by retesting.

c. When does testing take place in secure environments, if at all, and if it does, how?

Testing is conducted in a non-public facing environment with additional access controls.

d. How does your organization promote data quality and mitigate risks of harmful bias, including in training and data collection processes?

TELUS uses a unified risk assessment tool called the Data Enablement Plan (DEP) to identify the measures to promote data quality and mitigate harmful biases throughout the AI lifecycle. This includes requirements for data quality and metadata management in adherence to our Data Governance Framework and bias mitigation in adherence to our Responsible AI Framework. The DEP also identifies requirements for AI model governance in adherence to our Model Governance Standard.

e. How does your organization protect intellectual property, including copyright-protected content?

Team members are provided with Data & AI Literacy training and Guidance on Generative AI to help them understand how to safely and appropriately use generative AI, including what can be used and shared.

f. How does your organization protect privacy? How does your organization guard against systems divulging confidential or sensitive data?

TELUS is committed to being clear on how and when data is used and what controls exist to govern and manage those data uses. We are committed to sharing information about our data programs and practices by providing updates on our Trust Centre at https://www.telus.com/Trust. This is foundational to earning and maintaining our customers' trust. TELUS has a Privacy Policies and Commitments page which can be found at https://www.telus.com/en/about/privacy/

TELUS also publishes its robust Privacy Management Program Framework. The components set out in this document reflect TELUS' desire to exceed our privacy obligations as prescribed by legislation, to be transparent with customers, and to provide further direction for TELUS team members. See: https://www.telus.com/en/about/privacy/management-framework

Since 2019, TELUS has had a public commitment to Responsible AI, including describing examples of the way AI is used within the organization to help advance AI literacy and understanding of advanced AI systems. The development of this page was informed by user research and feedback. See: https://www.telus.com/ResponsibleAI

**g. How does your organization implement AI-specific information security practices pertaining to operational and cyber/physical security?
i. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems?
ii. How does your organization protect against security risks the most valuable IP and trade secrets, for example by limiting access to proprietary and unreleased model weights? What measures are in place to ensure the storage of and work with model weights, algorithms, servers, datasets, or other relevant elements are managed in an appropriately secure environment, with limited access controls in place?
iii. What is your organization's vulnerability management process? Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?
iv. How often are security measures reviewed? v. Does your organization have an insider threat detection program?
**

TELUS practices Secure by Design to build secure solutions in early stages of the project lifecycle through threat and risk identification as well as security control recommendations. Secure by Design (SbD) is a process that enables team members, business units and partners to learn about, implement and meet TELUS security standards. The security team provides resources to inform, verify and consult on engagement design, starting early in the process – intended to ensure security is built-in to all solutions, including AI, from the ground-up.

h. How does your organization address vulnerabilities, incidents, emerging risks?

TELUS is committed to security and protects cybersecurity with industry-leading best practices, a strong internal culture of security, and cutting-edge technology to safeguard information. Information about our security commitment is available here: https://www.telus.com/en/about/security/telus-commitment-to-security?intcmp=tcom_about_security_cont_telus-commitment-to-security

Any further comments and for implementation documentation

No answer provided

Section 3 – Transparency reporting on advanced AI systems

**a. Does your organization publish clear and understandable reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems?
i. How often are such reports usually updated?
ii. How are new significant releases reflected in such reports?
iii. Which of the following information is included in your organization's publicly available documentation: details and results of the evaluations conducted for potential safety, security, and societal risks including risks to the enjoyment of human rights; assessments of the model's or system's effects and risks to safety and society (such as those related to harmful bias, discrimination, threats to protection of privacy or personal data, fairness); results of red-teaming or other testing conducted to evaluate the model's/system's fitness for moving beyond the development stage; capacities of a model/system and significant limitations in performance with implications for appropriate use domains; other technical documentation and instructions for use if relevant.
**

In May 2024, TELUS launched a public-facing GenAI customer support tool which was first in the world to be internationally certified in Privacy by Design (ISO 31700-1).

The GenAI tool was evaluated by a third-party for alignment with international privacy criteria and the requirements laid out in the ISO 31700-1 Privacy by Design Standard. This achievement underscores our unwavering commitment to the highest standards of privacy and data protection, while continuously innovating to deliver a best-in-class customer experience.

As part of releasing this customer support tool, we developed a set of FAQs accessible through the user interface to help provide transparency on the capabilities and limitations of the system. This shares the capabilities and limitations of its generative AI customer support

system and the implications for the domains of appropriate use. See: https://www.telus.com/en/support/article/generative-ai-support-tool-faq.

TELUS shares information about its commitments to Responsible AI at: https://www.telus.com/ResponsibleAI.

Our TELUS Trust Model, published in 2015, guides all decision-making related to data and helps us build trust with our stakeholders by using data in ways that generate value, promote respect and deliver security(see www.telus.com/Trust). By putting our customers and communities first, the TELUS Trust Model reflects our commitment to earning trust through the protection of personal information in all of our data use and handling practices. We provide easy-to-access information on TELUS' privacy practices and how we use data at TELUS via the TELUS Trust Centre. For example, we have an easy-to-find summary on Responsible AI at TELUS on the Trust Centre (https://www.telus.com/Trust).

In addition, TELUS was one of the first organizations in the world to make our privacy management framework publicly available, having long understood that transparency is an important pillar of trust (https://www.telus.com/Privacy).

TELUS updates the information on these resources as it becomes available through system updates and new releases. Information about the use of AI is included in annual sustainability reporting: (https://www.telus.com/en/social-impact/caring-for-the-environment/sustainability-reports).

b. How does your organization share information with a diverse set of stakeholders (other organizations, governments, civil society and academia, etc.) regarding the outcome of evaluations of risks and impacts related to an advanced AI system?

TELUS participates in forums to develop, advance and adopt shared practices for ensuring the trustworthiness of AI including the NIST AI Safety Consortium, Responsible AI Institute, IAPP AI Governance (Foundational Supporter), the Standards Council of Canada National AI & Data Governance Standards Collaborative, Mila - Quebec Artificial Intelligence Institute, Alberta Machine Intelligence Institute (AMII) and Vector Institute.

c. Does your organization disclose privacy policies addressing the use of personal data, user prompts, and/or the outputs of advanced AI systems?

Yes, TELUS provides privacy statements that explain, in-depth, how TELUS collects, uses, discloses or otherwise processes personal information. These foundational privacy statements are sometimes supplemented with specific privacy notices that provide users with notification

of practices that are unique to a specific website, application or transaction, such as the use of AI to assist in decision–making. Information about privacy at TELUS can be found at https://www.telus.com/Privacy .

We also inform customers of what we are doing and provide easy-to-access information to help them understand TELUS' privacy practices and how we use data via the TELUS Trust Centre. For example, the use of AI is a concern for customers, so we have an easy-to-find summary on Responsible AI at TELUS on the Trust Centre (see https://www.telus.com/Trust).

d. Does your organization provide information about the sources of data used for the training of advanced AI systems, as appropriate, including information related to the sourcing of data annotation and enrichment?

Yes, clear guidance is included in the interface of our publicly-facing generative AI-powered customer support tool and is supplemented with detailed answers to potential questions (frequently asked questions) to further awareness and AI literacy for audiences. Guidance for use of generative AI is also provided to team members for our internal tooling to support understanding of how to use it safely and responsibly.

e. Does your organization demonstrate transparency related to advanced AI systems through any other methods?

Yes, with the rapid evolution of technology and the rise of AI we believe education in AI is critical for transparency. TELUS partnered with Canadian Institute for Advanced Research (CIFAR) to advance AI literacy in youth and more broadly through the Destination.AI course available for free online. See: https://cifar.ca/cifarnews/2023/11/17/open-call-for-high-school-students-participate-in-positively-ai-a-think-tank-by-cifar-and-telus/
https://cifar.ca/ai/destinationai/

In addition, our TELUS Wise program, which provides free training on digital safety, includes a new workshop on responsible AI to aid youth in navigating AI responsibly. See: https://www.telus.com/en/wise

TELUS also conducts public purple teaming events as a method of engaging diverse stakeholders in analyzing and assessing the fitness of generative AI systems for different purposes(for example, at the All In AI event in September 2024 https://allinevent.ai/).

Any further comments and for implementation documentation

No answer provided

Section 4 – Organizational governance, incident management and transparency

a. How has AI risk management been embedded in your organization governance framework? When and under what circumstances are policies updated?

TELUS has a dedicated Data & Trust Office (DTO), and all of the organization's data risk management and governance policies are based on the TELUS Trust Model which is posted publicly at https://www.telus.com/Trust . Furthermore, TELUS publicly committed to the responsible use of AI in 2019.

It is our objective to leverage our technology and our position as a global leader in social capitalism to collaborate with global thinkers and build a future where AI can deliver innovative and responsible social benefits.To support these public-facing commitments, TELUS has established an AI Policy for responsible governance and use of AI across the organization. It affirms TELUS' dedication to developing, using and deploying AI technologies in a way that drives positive change, while managing risks and ensuring appropriate safeguards are in place. The AI Policy requires that AI systems are used, developed, deployed, procured and provisioned in accordance with our Data Principles (see https://www.telus.com/Trust), our legal obligations and our Code of Ethics and Conduct (see https://www.telus.com/en/about/policies-and-disclosures/code-of-ethics-and-conduct).

Our Data Risk Management Policy and Framework is designed to align various stakeholders in data innovation and support risk identification at TELUS across the lifecycle of advanced AI systems. To support risk management and governance, a Data Enablement Plan (DEP) is required for AI initiatives. The DEP unifies our Responsible AI, Privacy Impact Assessment and Secure by Design, including cybersecurity, review processes into a single touchpoint and improves our agility through in-business data stewardship. To support enterprise adoption of generative AI, TELUS has a defined set of guidelines about how and where the technology can be used.

Policies are reviewed and updated annually to account for changing legislation and industry best practice. Our guidelines are updated regularly to support the evolving ecosystem of leading practices in managing AI risk and governance. This is guided by our enterprise data governance structure, including the cross-functional Responsible AI Squad.

b. Are relevant staff trained on your organization's governance policies and risk management practices? If so, how?

TELUS has a dedicated Data & Trust Office with over 50 privacy, data governance and data ethics professionals. This includes an in-house Data Ethicist and resources trained in ethical

machine learning techniques. Team members participate in external training, including the International Association of Privacy Professionals' AI Governance Professional certification. TELUS is a foundational sponsor of this program.

Across the organization, team members are appointed as Data Stewards by their business unit for their in-depth knowledge of their team's data uses and the intended strategy for that data. TELUS has over 500 data stewards who participate in a customized certification training program which equips and empowers the responsible use of AI through data privacy, security and governance. Across the AI lifecycle, business and technology teams are active participants in the identification, mitigation and acceptance of risk when using data with the support of TELUS' data governance processes. In addition, certified Data Stewards pursue additional external training and certification from the International Association of Privacy Professionals.

The Data & Trust Office also runs a data and AI literacy campaign for all team members to better understand both the opportunity of data and AI, but also the governance policies and risk management practices. This included partnering with Canadian Institute for Advanced Research (CIFAR) on the promotion of the Destination.AI literacy training program, and organizations like Microsoft and Google to share their learning resources.

More recently, immersive training has taken place through our TELUS Purple Team. We believe responsible use of AI requires input from a diverse set of voices. Through our purple teaming exercises, we invite any and all team members to participate in a collaborative exercise to identify weaknesses, vulnerabilities, and gaps in generative AI systems through adversarial testing and address them with relevant mitigations. In addition to the participation from the Software Developers, Data Scientists and AI Engineers, it emphasizes the participation of diverse individuals with varying expertise and technical literacy to gain comprehensive insights into the system's shortcomings and how real users may interact with the solution.

c. Does your organization communicate its risk management policies and practices with users and/or the public? If so, how?

TELUS has a dedicated site to sharing information about its risk management practices at https://www.telus.com/Trust .

d. Are steps taken to address reported incidents documented and maintained internally? If so, how?

TELUS has an incident readiness and response playbook that includes notification strategy and execution for the impacted customers, relevant stakeholders and regulators. Incidents are documented according to our incident management program.

e. How does your organization share relevant information about vulnerabilities, incidents, emerging risks, and misuse with others?

TELUS participates in forums to share relevant information about vulnerabilities, incidents, emerging risks and misuse such as the NIST AI Safety Consortium, Responsible AI Institute, Foundational Supporter of IAPP AI Governance, Standards Council of Canada National AI & Data Governance Standards Collaborative, Mila Quebec Artificial Intelligence Institute and Vector Institute.

f. Does your organization share information, as appropriate, with relevant other stakeholders regarding advanced AI system incidents? If so, how? Does your organization share and report incident-related information publicly?

TELUS has a data incident readiness and response playbook that includes notification strategy and execution for the impacted customers, relevant stakeholders and regulators. TELUS may share and report information related to material incidents publicly to the extent that it is required by law, or to the extent that it is permissible by law and in the public interest.

g. How does your organization share research and best practices on addressing or managing risk?

TELUS participates in forums to develop, advance and adopt shared practices for ensuring the trustworthiness of AI such as the NIST AI Safety Consortium, Responsible AI Institute, Foundational Supporter of IAPP AI Governance, Standards Council of Canada National AI & Data Governance Standards Collaborative, Mila Quebec Artificial Intelligence Institute, and Vector Institute.

h. Does your organization use international technical standards or best practices for AI risk management and governance policies?

TELUS aligns its AI governance program with international technical standards and best practices including ISO-41001; ISO-31700 and the OECD AI Principles. In May 2024, TELUS launched a public-facing GenAI customer support tool, which was first in the world to be internationally certified in Privacy by Design (ISO 31700-1).

TELUS is proud to be the first telecom in Canada to sign the Government of Canada’s voluntary code of conduct for generative AI, which seeks transparent, equitable and responsible development of GenAI technology in Canada. https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

TELUS is participating in the Standards Council of Canada National AI & Data Governance Standards Collaborative and working groups in the NIST AI Safety Consortium to help advance

the development and deployment of safe, trustworthy AI.

Any further comments and for implementation documentation

No answer provided

Section 5 – Content authentication & provenance mechanisms

a. What mechanisms, if any, does your organization put in place to allow users, where possible and appropriate, to know when they are interacting with an advanced AI system developed by your organization?

TELUS undertakes user experience research to identify opportunities to support comprehension of the limitations and capabilities of AI. This includes exploring design patterns which support trustworthy AI. For example, our public-facing generative AI support tool includes a statement and FAQs to support customer awareness of interactions with the AI system.

b. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems? If yes, how? Does your organization use international technical standards or best practices when developing or implementing content provenance?

Transparency is foundational for trust, as identified by our long-standing Trust Model, and for building trust in AI. TELUS provides users of AI with information to understand when content is generated by advanced AI systems, such as prominent placement of guidance on the use of AI on internal tools and FAQs on AI on our customer-facing GenAI, for example. We ensure that systems, which could be mistaken for humans, are clearly and prominently labelled as AI systems.

TELUS recognizes the challenges of addressing content provenance when using advanced AI systems. Generative AI is often trained on unknown image data sources. By using patterns and visual concepts obtained from the training data, the model can produce unique and realistic images. We work with our content development teams to build standards for how content generation is overseen by humans, and we collaborate closely with our communications teams to ensure that messaging around AI use is accurate and provides appropriate guidance and disclosures, thereby supporting data and AI literacy.

TELUS has been seeking input from a diverse set of voices about the hopes, opinions and concerns regarding AI. As part of this engagement, we have heard significant concerns from Indigenous Peoples about the impact of generative AI on Indigenous art, artists and visual representations of Indigenous Peoples. The generated images of Indigenous Peoples, such as

First Nations, Inuit and Métis Peoples, may perpetuate stereotypes, inaccuracies, and even offensive representations. With guidance from TELUS' Indigenous Advisory Council, TELUS declared publicly that it would not use AI to generate images or art of Indigenous Peoples.

https://www.telus.com/en/about/news-and-events/media-releases/telus-declares-it-will-not-use-ai-to-create-or-replicate-art-or-imagery-of-indigenous-peoples

Any further comments and for implementation documentation

No answer provided

Section 6 – Research & investment to advance AI safety & mitigate societal risks

a. How does your organization advance research and investment related to the following: security, safety, bias and disinformation, fairness, explainability and interpretability, transparency, robustness, and/or trustworthiness of advanced AI systems?

We believe responsible use of artificial intelligence (AI) requires input from a diverse set of voices. With a human-centred approach, we can build trust in our digital world and make a friendly future for all. Our inaugural annual AI report shared the views from thousands of people on AI - their concerns, hopes and opinions about where this powerful technology should be headed. This report is available to the public at: https://www.telus.com/ResponsibleAI.

b. How does your organization collaborate on and invest in research to advance the state of content authentication and provenance?

TELUS is actively participating and supporting initiatives from research institutes, organizations and universities to support GenAI safety, including content authentication. This includes the NIST AI Safety Consortium, Responsible AI Institute, Foundational Supporter of IAPP AI Governance, Standards Council of Canada National AI & Data Governance Standards Collaborative, Alberta Machine Intelligence Institute (AMII), Mila - Quebec Artificial Intelligence Institute and Vector Institute.

c. Does your organization participate in projects, collaborations, and investments in research that support the advancement of AI safety, security, and trustworthiness, as well as risk evaluation and mitigation tools?

TELUS is a member of the International Association of Privacy Professionals, and a founding sponsor of both the IAPP AI Governance Centre and the Canadian Anonymization Network

(CANON).

TELUS is actively participating and supporting initiatives from research institutes, organizations and universities to support GenAI safety. This includes the NIST AI Safety Consortium, Responsible AI Institute, Foundational Supporter of IAPP AI Governance, Standards Council of Canada National AI & Data Governance Standards Collaborative, Alberta Machine Intelligence Institute (AMII), Mila - Quebec Artificial Intelligence Institute and Vector Institute.

d. What research or investment is your organization pursuing to minimize socio-economic and/or environmental risks from AI?

In addition to our collaborative purple teaming efforts detailed above, TELUS is committed to incorporating the perspectives of Indigenous Peoples in its data ethics strategy and is undertaking engagements to learn more about where AI could be used to support Indigenous rights. With guidance from TELUS' Indigenous Advisory Council, TELUS declared in June 2024 that it would not use AI to generate images or art of Indigenous Peoples. https://www.telus.com/en/about/news-and-events/media-releases/telus-declares-it-will-not-use-ai-to-create-or-replicate-art-or-imagery-of-indigenous-peoples

Any further comments and for implementation documentation

No answer provided

Section 7 – Advancing human and global interests

a. What research or investment is your organization pursuing to maximize socio-economic and environmental benefits from AI? Please provide examples.

TELUS has developed a Canadian Sovereign AI Factory, powered by 99% renewable energy sources and featuring intelligent cooling to deliver AI as a Service (AIaaS). These data centres are designed to be three times more energy efficient for excess power usage than the industry average, using significantly less electricity to power AI computing workloads. The facilities also rely on natural cooling, cutting water consumption by more than 75% compared to traditional data centres. With these efficiency measures in place, TELUS' Sovereign AI Factory will be one of the most sustainable AI-ready data centres in the world.

TELUS' AI Factory will help Canada develop domestic AI technologies, increase productivity, protect data and support businesses, making the country economically competitive and future-ready.

We believe responsible use of AI requires input from a diverse set of voices. We have engaged with academic and research institutions to help drive out this research. Our annual TELUS AI Report shared the views from thousands of people about their thoughts on AI - their concerns, hopes and opinions about where this powerful technology should be headed. The report is made available publicly at: www.telus.com/ResponsibleAI

b. Does your organization support any digital literacy, education or training initiatives to improve user awareness and/or help people understand the nature, capabilities, limitations and impacts of advanced AI systems? Please provide examples.

With the rapid evolution of technology and the rise of AI we believe education in AI is critical for transparency. TELUS partnered with Canadian Institute for Advanced Research (CIFAR) to advance AI literacy in youth and more broadly through the Destination.AI course available for free online. In addition, our TELUS Wise program which provides free training on digital safety includes a new workshop on responsible AI to aid youth in navigating AI responsibly.

https://cifar.ca/cifarnews/2023/11/17/open-call-for-high-school-students-participate-in-positively-ai-a-think-tank-by-cifar-and-telus/
https://cifar.ca/ai/destinationai/

We believe responsible use of artificial intelligence (AI) requires input from a diverse set of voices. We have worked with an Indigenous owned software company, PLATO Consulting to set up an extended purple team and support Indigenous AI workforce capacity and skill-building. TELUS also conducts public purple teaming events as a method of engaging diverse stakeholders in analyzing and assessing the fitness of generative AI systems for different purposes(for example, at the All In AI event in September 2024 (https://allinevent.ai/).

In addition, our TELUS Wise program, which provides free training on digital safety, includes a new workshop on responsible AI to aid youth in navigating AI responsibly. See: https://www.telus.com/en/wise

c. Does your organization prioritize AI projects for responsible stewardship of trustworthy and human-centric AI in support of the UN Sustainable Development Goals? Please provide examples.

TELUS has participated in multiple projects with our research partner, the Vector Institute. For example, TELUS and the Vector Institute collaborated on an energy optimization system for the reduction of electricity consumption in data rooms. This work involved the application of model based reinforcement learning to leverage “free cooling” which is less energy intensive than traditional compressor-based air conditioning. Our pilot testing showed a decrease in ~20% electricity consumption in hot summer months. Link to this work can be found here:

https://vectorinstitute.ai/a-telus-ai-agent-approached-sustainability-like-a-chess-game-and-may-have-just-innovated-its-way-to-major-new-energy-savings/. We have open sourced the reference implementation for others to explore and apply in their small data settings. The GitHub repo can be found here: https://github.com/VectorInstitute/HV-Ai-C

d. Does your organization collaborate with civil society and community groups to identify and develop AI solutions in support of the UN Sustainable Development Goals and to address the world's greatest challenges? Please provide examples.

TELUS has participated in multiple projects with our research partner, the Vector Institute. These include:

- Analysis of social media to identify Long Covid symptoms: TELUS worked with the Vector Institute to identify COVID longhaul symptoms from social media posts using natural language processing techniques. This work was done in 2021. This was more recently published in the Journal of Medical Internet Research (September, 2023):https://www.jmir.org/2023/1/e45767
- Application of computer vision and generative AI to monitor vegetation health: TELUS worked with the Vector Institute on the SegMate toolkit drives groundbreaking AI solutions in the fight against climate change. SegMate enables state-of-the-art computer vision models to analyze satellite imagery for critical climate applications, including: Deforestation Monitoring: Track and manage forest health; Agricultural Land Use Analysis: Optimize land use for sustainability; Ocean and Water Body Analysis: Safeguard water ecosystems; and Natural Disaster Response: Improve preparedness and response to natural calamities. The GitHub repo can be found here: https://github.com/VectorInstitute/SegMate

Any further comments and for implementation documentation

No answer provided