

OECD AI Transparency Report

Organization: TELUS (CAN)

Reporting Period: Q3 2026

Published: October 2, 2026

Section 0 – Your role in the AI system lifecycle

Responding as (please select all that apply):

- Application developer (/provider)
- Deployer

If any of the fields above are selected, please indicate your organization size:

Large enterprise: 250 or more employees

Section 1 – Risk Identification and Evaluation

1. How does your organization define and/or classify different types of risks related to AI?¹

- Maintain an internal taxonomy, classification system, and/or set of risk area definitions
- Align with specific external frameworks, standards, reports, and/or guidance documents such as taxonomies, classification systems, and/or sets of definitions for risk areas (e.g. the NIST AI Risk Management Framework, the ISO/IEC 42001, the OECD AI Principles, the EU General-Purpose AI Code of Practice, the International AI Safety Report). (please specify):
NIST AI Risk Management Framework, ISO/IEC 31700-1, OECD AI Principles, Government of Canada Voluntary Code of Conduct for Generative AI, Government of Canada Voluntary Code of Conduct for Generative AI, Canada's Responsible Data Centre Development Principles.
- Consult with external stakeholders (e.g., from academia, industry groups, civil society, or standard development organisations) when developing or updating risk taxonomies

File IX

How does your organization define thresholds at which severe risks, unless adequately mitigated, may be considered "unreasonable"? Please describe the framework(s) most relevant to your organization's role and context. If your organisation does not use formal thresholds, you may describe instead the policies, decision criteria, or governance processes you apply when assessing severe AI risks. You may also describe:

- Specific examples of contexts in which your models or systems could, in your assessment, pose unreasonable or intolerable risk;
- How mitigations are graduated by capability or propensity level;
- How your organisation considers the specificities of different AI technologies, such as generative AI and agentic AI, including any specific risk assessment or governance mechanisms applied to agentic AI capabilities.

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 (DEP) 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 governs AI risk via its enterprise Data Risk Management Policy and Framework. Risk thresholds determine the level of executive decision-making and acceptance required. Risk classification under this framework determines not only the level of executive oversight required for acceptance, but also the intensity and type of mitigations applied across the AI lifecycle.

Under our AI Policy and Code of Ethics and Conduct (see: <https://www.telus.com/en/about/policies-and-disclosures/code-of-ethics-and-conduct>), TELUS strictly prohibits deployment under specific "unreasonable risk"

scenarios, including but not limited to: Subliminal or manipulative techniques distorting informed decision-making; Exploitation of vulnerable groups based on age, disability, or socio-economic status; and AI-generated art or imagery replicating Indigenous Peoples (guided by our Indigenous Advisory Council) (see: <https://www.telus.com/en/about/trust/responsible-ai/image-generation-declaration>). TELUS uses, develops, deploys, procures and provisions AI Systems in accordance with our Data Principles (see <https://www.telus.com/Trust>). All AI systems, regardless of type, are evaluated through our Data Enablement Plan (DEP) process, which unifies risk assessment for Responsible AI, Privacy Impact Assessment, and Secure by Design considerations across the entire AI lifecycle. TELUS has also developed Responsible Agentic AI guidelines to address the specific governance requirements of agentic AI systems.

2. Both before and after deployment, what practices does your organization use to identify and evaluate vulnerabilities, incidents, emerging risks and misuse throughout the AI system lifecycle?

- Internal red teaming³
- Independent third-party red teaming
- Adversarial testing to detect technical vulnerabilities
- Publicly available benchmarks and measurement tools
- Internal benchmarks, standard metrics (e.g., frequency, severity scores)
- Structured techniques to explore the behavior or performance of a model and/or application, such as model elicitation or bottleneck assessments
- Qualitative assessments (e.g., expert judgment, narrative scoring)
- Specific risk identification practices for vulnerable groups
- Impact assessments such as personal data protection assessment and fundamental rights impact assessments
- Internal model, system, or application-independent research initiatives
- External model, system, or application-independent research initiatives
- Vulnerability reports
- Incident reports, including reports shared by other organizations
- Automated monitoring / remote status reporting (e.g., telemetry pipelines, automated alerts when risk thresholds are breached)
- Specific risk identification practices for agentic AI capabilities, e.g., autonomous action-taking, tool use, multi-step planning (please specify): 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, including interactions by and between AI systems, as applicable. In addition, TELUS co-founded the AI Consortium with Lightworks, Scotiabank, and Sun Life to build critical AI control infrastructure in Canada. The AI Consortium's flagship program, the Agentic Control Plane (ACP), is already running in production in regulated environments. The ACP gives enterprises the visibility and control needed to manage Agentic AI at scale, across models, agents, users and inference pipelines. It helps support regulatory compliance, maintain operational control and currently processes more than two trillion tokens per month across member organizations. See: <https://www.telus.com/en/about/news-and-events/media-releases/Lightworks-Scotiabank-Sun-Life-and-TELUS-launch-AI-Consortium-to-jointly-build-critical-AI-control-infrastructure-in-Canada>
- Assessment of risks arising from interactions among multiple AI agents
- Multilingual and cross-cultural evaluation, including collaboration with local ecosystems (e.g., national AI institutes, language-specific evaluation consortia) for under-represented languages and cultural contexts (please specify): TELUS recognizes that responsible AI development requires understanding how AI systems affect a wide variety of communities and people. To ensure our AI tools are safe, fair, and respectful across diverse populations, TELUS actively seeks input from people with varied backgrounds, experiences, and identities about how our systems perform and impact their communities. 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. Generated images of Indigenous Peoples - including First Nations, Inuit, and Métis Peoples - may perpetuate stereotypes, inaccuracies, and offensive representations. In response, and with guidance from TELUS's Indigenous Advisory Council, TELUS publicly committed not to use AI to generate images or art depicting Indigenous Peoples. To advance responsible and culturally-informed AI

evaluation practices, TELUS conducts purple teaming exercises that bring together people from diverse backgrounds, experiences, and identities to test how AI tools respond to and serve different communities. This approach helps identify potential harms, biases, and gaps that may not be apparent through traditional testing methodologies. Additionally, TELUS partnered with wâsikan kisewâtisiwin, an Indigenous-led AI startup whose AI writing tool helps identify cultural bias and inaccuracies in writing about Indigenous Peoples. TELUS is the first beta tester for this tool.

Are any national AI safety / security institutes of the AISI network involved?

No

How does your organization monitor the interactions of AI agents under your control with other agents / assess risk from multiple agents interacting?

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, including interactions by and between AI systems, as applicable. In addition, TELUS co-founded the AI Consortium with Lightworks, Scotiabank, and Sun Life to build critical AI control infrastructure in Canada. The AI Consortium's flagship program, the Agentic Control Plane (ACP), is already running in production in regulated environments. The ACP gives enterprises the visibility and control needed to manage Agentic AI at scale, across models, agents, users and inference pipelines. It helps support regulatory compliance, maintain operational control and currently processes more than two trillion tokens per month across member organizations. See: <https://www.telus.com/en/about/news-and-events/media-releases/Lightworks-Scotiabank-Sun-Life-and-TELUS-launch-AI-Consortium-to-jointly-build-critical-AI-control-infrastructure-in-Canada>

Please briefly describe your organization's decision-making process for deploying an AI model or system including: who has decision authority; what evidence and criteria are required (e.g., performance, safety/security, robustness, fairness, privacy, compliance, independent external testing, evaluation, validation and verification (TEVV) or assurance); contextual caveats or limitations required in interpreting risk evaluation metric results; what approvals/sign-offs are needed; and what safeguards (e.g., mitigations, monitoring, or phased release) must be in place to move into deployment.

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 (DEP) 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.

Systems undergo cross-functional Purple Teaming (collaborative adversarial testing involving developers, data scientists, engineers, and non-technical staff) based on risk level. Testing reports cover methodology, key findings, and unmitigated risks. For sign-off of AI risks, risk acceptance procedures align with the Data Risk Management Policy, supported by in-business Data Stewards and the Data & Trust Office (DTO)

Following deployment, how do you use incident reports — including those shared by other organizations — to identify emerging issues, update risk assessments, and trigger corrective actions.

TELUS integrates feedback loops within user interfaces and maintains support lines for reporting vulnerabilities, and has an incident readiness and response playbook that includes notification strategy and execution for the impacted customers, relevant stakeholders and regulators. Reports are processed under the incident readiness and response playbook to trigger updates to risk assessments and initiate corrective mitigation and/or re-testing.

3. Does your organization have mechanisms to receive and/or share reports of risks, incidents or vulnerabilities by/with third parties?

Yes, both receiving and sharing

If yes, please indicate which stakeholders reporting mechanisms may be accessible to, recognising specifics will depend on the nature of the report and risk level. For each, indicate whether access is on a standing basis (Always), activated based on context (Ad hoc/as relevant), or not currently accessible.

	Always	Ad hoc / as relevant	Not currently accessible
Relevant employees (security, legal/compliance, etc.)	☐		
Public authorities (e.g., public reporting offices for security incidents or data breaches)		☐	
Supervisory authorities (e.g., data protection authorities)		☐	
Industry partners or industry fora		☐	
Users (end users, enterprise customers, developers using APIs)	☐		
Business customers / deploying organizations (if different from “users”)		☐	
Supply-chain partners (cloud, data providers, etc.)		☐	
Academia / researchers		☐	
Independent auditors		☐	
Standards bodies / multi-stakeholder initiatives (OECD.AI, ISO/IEC, IEEE, etc.)		☐	
Specific civil society organizations		☐	
Media / general public (people or communities indirectly impacted)		☐	
Other			

Please describe how your organisation determines when and how reporting mechanisms are made accessible to different stakeholders (e.g. based on legal or regulatory requirements, internal policies, or risk level). Please also provide public URLs or details on how to submit reports. If none, write “Not applicable”

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 and accessible to relevant stakeholders as-required. 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. Reporting of AI incidents are required by our AI policy, and reporting is further 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.

Public URLs for information on reports: telus.com/Trust, telus.com/ResponsibleAI.

How does your organization share relevant information as appropriate?

- Publicly
- Information-sharing partnerships (with confidentiality agreements as appropriate)
- Reporting to regulatory authorities as relevant

Please describe what type of information is shared.

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

4. If your organization has programs to incentivize risk(s) disclosure, incidents and systemic vulnerabilities, please share what type of programs you use?

- Internal incentives and culture

Please provide public URLs and/or details on your incentive program(s). If none, write “Not applicable.”

Not applicable

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

Contributes and uses

If contributes or uses, please select all that apply:

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005)
- NIST AI Risk Management Framework (AI RMF)
- Industry-led best practices or codes of conduct
- OECD Due Diligence Guidance for Responsible AI
- Other international or regional standards (please specify): Voluntary Code of Conduct on the Responsible Development and Deployment of Generative AI, Canada’s Responsible Data Centre Development Principles

6. Does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks that could have broad and potentially cascading socio-economic impacts? Please indicate which stakeholders you collaborate with, and whether collaboration is on a standing basis (Always-on), activated based on context (Ad hoc/as relevant), or there is no current collaboration.

	Always-on	Ad hoc / as relevant	No current collaboration
Relevant employees (security, legal/compliance, etc.)	☐		
Public authorities / regulators / AI safety institutes / other public sector bodies and inter-governmental coordination structures	☐		
Industry partners or industry fora	☐		
Users (end users, enterprise customers, developers using APIs)	☐		
Business customers / deploying organizations (if different from “users”)		☐	
Supply-chain partners (cloud, data providers, etc.)		☐	
Academia / researchers	☐		
Independent auditors		☐	
Standards bodies / multi-stakeholder initiatives (OECD.AI; ISO/IEC; IEEE; AIID etc.)		☐	
Independent civil society organizations (e.g., for evaluations, audits, or policy review)		☐	
Media / general public (people or communities indirectly impacted)	☐		
Other(s) (please add any other relevant stakeholder groups):			
Not applicable			

Please describe examples of how your organization collaborates. Examples may include: participating in multi-stakeholder or industry initiatives; partnering with academia, civil society, or the public sector; establishing internal or joint governance structures with external experts or in partnership with other efforts to share knowledge and jointly address risks.

TELUS participates in international standards initiatives including the Hiroshima AI Process (HAIP) Reporting Framework, where it was the first Canadian company to contribute, the Thompson Reuter's Foundation AI Company Data Initiative, the NIST AI Safety Consortium, the Government of Canada's Voluntary Code of Conduct for Generative AI, which TELUS was the first telecom in Canada to sign, and Canada's Responsible Data Centre Principles.

TELUS partners with academic institutions such as the Vector Institute on AI research projects addressing sustainability and health challenges, with findings and implementations shared publicly. TELUS also collaborates with the Canadian Institute for Advanced Research (CIFAR) to advance AI literacy through free online courses and youth training programs. Furthermore, TELUS is a proud partner of the SSHRC-funded Algorithmic Bias in Canada (ABC) project, hosted by the University of Toronto's Centre for Ethics. This interdisciplinary collaboration, which includes the Schwartz Reisman Institute and the Chiefs of Ontario, allows TELUS to collaborate with leading philosophers and researchers to identify and mitigate algorithmic bias, directly addressing the socio-economic risks of AI discrimination. (See: <https://srinstitute.utoronto.ca/news/when-the-algorithm-is-wrong>)

Internally, TELUS uses a cross-functional purple teaming approach where developers, data scientists, and diverse cross-functional team members conduct adversarial testing to identify vulnerabilities in AI systems. TELUS also works with Indigenous-owned companies and partners such as pipikwan pêhtâkwan to embed Indigenous perspectives into AI design and governance.

TELUS co-founded the AI Consortium with Lightworks, Scotiabank, and Sun Life to build critical AI control infrastructure in Canada. The Consortium enables members to pool engineering expertise, conduct deep research, and jointly build and govern mission-critical AI control systems and intellectual property, with resulting IP deployed individually and available to members through perpetual-use and ownership rights.

Finally, TELUS conducts annual public engagement through its TELUS AI Report, surveying thousands of Canadians and Americans to inform its responsible AI approach and share public perspectives on AI governance.

Any further comments and implementation documentation.

No answer provided

Section 2 – Risk Management and Information Security

7. Across the AI system lifecycle, what steps does your organization take to manage risks and vulnerabilities? Please indicate which specific practices, tools or metrics your organization uses at each lifecycle stage. You may refer to tools or metrics present in the OECD.AI Catalogue of Tools and Metrics or suggest additions. Respondents may complete only the lifecycle stages relevant to their organisation's role. Stages that do not apply may be left blank.

Plan and design

Collect and process data

Build, integrate and interpret model

Verify and validate

Deploy

Operate and monitor

Please provide a consolidated description of your organisation's approach to risk management across the AI system lifecycle, including how the practices identified above operate together and any cross-cutting governance, review or escalation processes. Please also indicate how often these practices are reviewed and what types of events trigger

reviews and updates. Where relevant, please distinguish between different types of AI systems (e.g. generative or agentic AI).

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 and is embedded by the Data Enablement Plan, which functions as a single entry point for Privacy, Security, and Ethical AI governance. Policies are reviewed regularly and are further triggered by new regulatory standards and system updates in the markets where TELUS operates.

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.

Please describe any measures used to ensure data quality and fairness across the data collection and curation stage (e.g., dataset audits, filtering training data to remove harmful content or personal information, fine-tuning on curated data, use of moderation tools, assessment of limitations to model generalisability).

TELUS utilizes its unified risk assessment tool, the Data Enablement Plan (DEP), which identifies specific measures to promote data quality and mitigate harmful biases. This process enforces requirements for data quality and metadata management. TELUS also leverages a collaborative purple teaming approach, engaging diverse individuals with varying expertise and technical literacy in adversarial testing to identify weaknesses, vulnerabilities, and gaps in generative AI systems and address them with relevant mitigations.

8. What security measures are used in testing AI systems?

- Isolated and secure test environments
- Network isolation from external access
- Isolation of staging environments (from production / operational environments)
- Controlled environments for red-teaming and adversarial testing
- Containment measures for prompt-injection and jailbreak attempts
- Controlled security vulnerability testing
- Rate limits and resource caps
- Human-in-the-loop controls for higher-risk test cases
- Access controls, including roles-based permissions
- Audit logging and monitoring
- Use of "AI-safe" test-data, as appropriate
- Use of synthetic, anonymized, or dummy data, as appropriate

8.A. Please indicate, if relevant, the team or role responsible for overseeing secure testing and whether this responsibility is shared across multiple teams and/or functions.

Multiple teams are involved in securing testing, including teams for test data management, security testing teams, purple teams where necessary, and quality assurance, among others.

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

9.A. Safeguards that promote lawful data use and transparency in AI training:

- Maintain a copyright policy that addresses data sourcing, content provenance, safeguards, and organizational roles and responsibilities
- Publishing "model cards" or contextual information on training data and model limitations

- Refrain from the unlawful circumvention of technological protection measures in data sourcing
- Conduct data cleaning, qualification, and/or tokenization activities as part of a transformative data preparation process
- Consult and/or retain an intellectual property attorney to protect, enforce, and comply with, intellectual property rights.

9.B. Safeguards that reduce the risk of dissemination of outputs that may infringe copyright:

- Restricting outputs that raise ethical, human rights, or legal concerns—such as non-consensual intimate imagery, unauthorized deepfakes, or outputs that are substantially similar to copyrighted works.

10. How do you protect privacy and prevent your systems from disclosing confidential or sensitive data across the AI lifecycle?

- Make information about data privacy, practices, and controls accessible to a diverse set of stakeholders
- Use security controls, including encryption at rest and in transit
- Provide organizational customers with controls to configure and implement privacy choices (e.g., data retention, logging, access, or processing settings)
- Apply Privacy-Enhancing Technologies (PETs) where applicable (e.g. differential privacy, federated learning, synthetic data generation, homomorphic encryption)

Describe key privacy measures and data-protection standards applied.

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/>, and has enterprise alignment with ISO 31700-1 (Privacy by Design).

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>

11. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems across the AI system lifecycle? Respondents may complete the checkbox subsections in 11.A–11.D or describe their overall approach under 11.E.

11.A. Governance, policy and assessments

- Conduct regular cybersecurity risk and vulnerability assessments tailored to AI models or systems
- Perform threat modeling that includes AI-specific risks (e.g., data poisoning, prompt injection)
- Maintain or update security policies aligned with recognized standards (e.g., NIST CSF, ISO/IEC 27001, SOC 2, CIS Critical Security Controls), and review them regularly in response to emerging risks or regulatory guidance
- Maintain vulnerability management processes (scanning, channels for external reporting, patching, remediation)
- Implement incident response, disaster recovery, or business continuity plans, including escalation procedures for high-severity incidents
- Train staff on cybersecurity best practices and AI-specific threats, including how to recognize and respond to misuse or unintended outcomes of advanced AI systems
- Integrate cybersecurity AI risks into broader cybersecurity risk management activities
- Regularly review security measures and update them in response to emerging risks, incidents, or major releases

11.B. Technical and operational controls

- Apply multi-factor authentication (MFA) and role-based access controls for advanced AI systems
- Encrypt AI assets (datasets, models, configurations) in storage and in transit as appropriate
- Restrict physical access to servers, GPUs, or devices hosting AI models, systems, and/or applications
- Monitor system activity and log access to detect anomalies or misuse
- Conduct secure AI development and/or deployment practices
- Conduct security testing focused on AI-specific risks (e.g., red-teaming, adversarial testing, stress tests)

11.C. Protection of sensitive or high value AI assets

- These responsibilities are delegated contractually to model or infrastructure providers

11.D. Insider risk protection detections

- Conduct pre-employment screening or role-sensitive vetting
- Monitor for unauthorized internal access or suspicious activity
- Provide staff training on cybersecurity best practices and AI-specific threats
- Implement insider-risk escalation or response procedures

11.E. Please describe the main security measures your organization applies and indicate which are specific to particularly sensitive AI assets, where relevant.

TELUS operates a robust security program for new initiatives to embed security, privacy, and data governance at the early stages of development. We are actively engaged in adapting to the needs of AI-enabled solutions, including management of non-human identities, identity assurance, secrets management, least-privilege access, logging and monitoring, encryption in transit and at rest, vulnerability management, and security testing.

12. 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?

- Investigation of reported or identified risks and vulnerabilities
- Development of patches or other mitigations for confirmed risks or vulnerabilities
- Testing of patches or other mitigations
- Scanning for and mitigation of similar risks or vulnerabilities
- Defined escalation criteria and follow-on actions for identified vulnerabilities (e.g., for external reporting or information sharing)
- Reporting to regulators / authorities when relevant

13. What post-deployment practices does your organization use to monitor and respond to vulnerabilities, incidents, emerging risks and misuse of advanced AI systems?

- Conduct post-deployment monitoring
- Perform root-cause analysis and apply lessons learned to improve future development and/or deployment practices

14. Do you develop or deploy agentic AI systems (systems that can autonomously plan/act or use tools)?⁴

Yes

14.A. If yes, please indicate which categories of controls your organization applies. Please select all.

- Constraints on the agent's action space (e.g., tool-use permissions, environment sandboxing, allowlists/blocklists of resources, scope limits per task)
- Human oversight or interruptibility mechanisms (approval requirements for sensitive actions, escalation paths, interruption interfaces)
- Monitoring (anomaly detection, multi-agent interaction monitoring)
- Logging of agent actions

Please provide any further comments and implementation documentation.

No answer provided

Section 3 – Transparency Reporting on Advanced AI Systems

15. Does your organization publish public reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems? Are these clear and understandable by non-technical audiences?

Yes

15.A. If yes, which of the following information is included in your organization's publicly available documentation for any of your AI products?

- Risk management policies
- Capabilities, behaviours, and limitations, including domains of appropriate and inappropriate use or indicative thresholds associated with systemic risks.
- Plain-language or non-technical summaries

Please provide links or references showing where this information is made public.

<https://www.telus.com/en/support/article/generative-ai-support-tool-faq>

<https://www.telus.com/ResponsibleAI>

<https://www.telus.com/Trust>

<https://www.telus.com/Privacy>

<https://www.telus.com/en/social-impact/caring-for-the-environment/sustainability-reports>

15.B. If yes, how often are such reports usually updated?

Other (e.g., triggered by material changes, incidents, or new risks)

16. 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?

- Public documentation
- Protected information sharing
- Regulatory reporting as relevant
- Direct engagement with AI safety institutes, civil society or academic partners

Describe how evaluation results are shared and with which stakeholders (e.g. other organizations, governments, civil society and academia, etc). You may also indicate whether non-technical or plain-language summaries are provided for broader audiences.

TELUS maintains a dedicated public-facing resource at www.telus.com/ResponsibleAI that shares information about its commitments to responsible AI. This includes the TELUS Trust Model, which guides all decision-making related to data and AI.

TELUS provides dedicated FAQs where relevant that include information about AI system limitations and capabilities. These FAQs may be embedded directly in products (such as Smart Home+ AI Assistant) as well as being made available online where applicable (for example, the GenAI FAQ at <https://www.telus.com/en/support/article/generative-ai-support-tool-faq>). This approach ensures that users encounter relevant information about AI systems at the point of use while also maintaining centralized online resources.

TELUS Digital published its GenAI Safety Model Benchmark, testing 34 AI models from 10 global providers across 620,000+ adversarial attack simulations. The full report is publicly available at <https://www.telusdigital.com/insights/fuel->

[ix/resource/genai-safety-benchmark-2026](#) and includes detailed vulnerability rates, model rankings, and analysis of safety factors.

TELUS also publishes an annual AI Report made available publicly at www.telus.com/ResponsibleAI that includes findings from thousands of respondents about public perception of AI capabilities, limitations, and appropriate use.

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

Yes

If yes, provide links to privacy policies or notices covering personal data, user inputs, and AI-generated outputs.

<https://www.telus.com/en/about/privacy/commitment>

<https://www.telus.com/Trust>

18. How 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?

- Public documentation
- Regulatory reporting as relevant

Please provide links to any publicly available information.

<https://www.telus.com/en/about/trust>

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

Yes

If yes, describe additional method(s), including where relevant transparency measures related to AI agents

TELUS actively participates in voluntary disclosure forums and initiatives to help set industry benchmarks. This includes the AI Company Data Initiative (AICDI) by the Thomson Reuters Foundation, where TELUS provides data on its AI governance and usage to enable broader industry transparency and risk mitigation.

TELUS engages in clear disclosure of AI interaction. We ensure that users are informed when they are interacting with an AI agent rather than a human representative, maintaining trust and clarity in the customer experience. This is further supported by comprehensive, accessible FAQs that clearly explain how AI is being used, what data is processed, and the purpose of the AI system in that specific interaction.

20. Does your organization publish statistical insights derived from anonymised, aggregated usage data to advance understanding of AI adoption and its economic impacts in areas including occupations and tasks by region, sector and country? To this end, do you contribute to international cooperation efforts?

Yes

If yes, please provide links or describe the scope of insights published, including where relevant contributions to understanding AI adoption in specific sectors (e.g. public administration, education systems).

TELUS contributes to the understanding of AI adoption and its societal impact through the publication of annual public sentiment research on AI, most recently in the 2026 TELUS AI Trust Atlas. The annual TELSU AI Report is a comprehensive, cross-border research study (surveying over 11,000 participants across Canada and the United States) that provides statistical insights into:

- Adoption Rates: Quantifying the prevalence of AI usage among the general public
- Trust & Human-AI Interaction: Analyzing how confidence in AI decision-making varies based on the presence of human supervision.

- Cross-Border Trends: Providing data from both the Canadian and American markets regarding AI trust, regulation, and expectations.

These insights are published in TELUS's annual AI reports and public media releases, contributing to the broader international dialogue on how to bridge the "trust gap" and ensure the responsible adoption of AI across different demographics and regions. More here: <https://www.telus.com/ResponsibleAI>

Please estimate the total staff time and annual expenses associated with conducting compliance activities and include any further comments and implementation documentation (optional).

No answer provided

Section 4 – Organizational Governance, Incident Management, and Transparency

21. How has AI risk management been embedded in your organization's governance framework?

- Board of Directors oversight
- Executive oversight
- Senior management oversight
- Governance council or committee
- Other (e.g., distributed / multi-institutional governance arrangement) (please specify): distributed through a network of in-business data stewards

Please describe how AI risk management is integrated into governance structures, including: which roles or bodies have advisory versus decision-making authority; which roles or bodies have final accountability for AI risk-related decisions; and how often policies are reviewed or updated (e.g., following major incidents, regulatory changes, or material updates to systems).

The TELUS 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. The DEP process is initiated by a certified Data Steward within the specific business unit who gathers details on the data or AI initiative. They then share these details with expert Data & Trust Office and Security team members who identify risks and establish mitigation plans. The process concludes with a formal sign-off from a sponsoring leader (director or above).

To support enterprise adoption of generative AI, TELUS has a defined set of guidelines about how and where the technology can be used. The responsible governance and use of AI across the organization is formalized in the TELUS AI Policy, which is approved and endorsed by the TELUS Board of Directors

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.

22. Are relevant staff trained on your organization's governance policies and risk management practices?

Yes

If yes, describe training methods (e.g., onboarding modules, regular sessions, and confidential channels to report concerns).

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. TELUS also offers OCAP® (Ownership, Control, Access, and Possession) training for TELUS team members who support data privacy, ethics, governance and AI in order to deepen understanding of Indigenous data sovereignty.

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.

Immersive training also takes 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. Before sessions begin, participants receive training on AI fundamentals and potential risks, ensuring everyone can contribute meaningfully regardless of technical background. Beyond finding vulnerabilities, these hands-on sessions help participants understand how AI works, how it can fail, and why responsible AI development matters. This creates a ripple effect of AI literacy and awareness throughout TELUS, building a more informed workforce that can better navigate an AI-enabled future.

23. Are steps taken to address reported incidents documented and maintained internally?

Yes

If yes, describe how incident records are kept and used for follow-up (e.g., incident logs, root-cause analysis reports, internal tracking systems). You may indicate whether and how you define escalation thresholds for when incidents must be surfaced to senior leadership or external parties.

TELUS has implemented an incident response process by which AI incidents are managed through their lifecycle, and which brings together appropriate stakeholders, depending on severity, to assess, contain, and remediate AI incidents and provide notification of such as needed. An "AI incident" is an event resulting in suspected or actual harm from the development or use of an AI system.

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.

24. Does your organization share research and best practices on addressing or managing risk?

Yes

If yes, describe how research or good practices are shared (e.g., publications, conferences, collaborations with other sectors).

TELUS participates in forums to share relevant information about vulnerabilities, incidents, emerging risks and misuse such as the NIST AI Safety Consortium, Foundational Supporter of IAPP AI Governance, Standards Council of Canada

National AI & Data Governance Standards Collaborative, Mila Quebec Artificial Intelligence Institute and Vector Institute. Responsible AI policies developed by TELUS are also shared publicly, discoverable at <https://www.telus.com/en/about/trust/responsible-ai>

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

Yes

If yes, please indicate which standards or frameworks apply:

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001)
- NIST AI Risk Management Framework (AI RMF)
- OECD AI Principles
- Industry-led best practices or codes of conduct

If yes, describe which international technical standards or best practices your organization uses.

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, IAPP AI Governance Global (Foundational Supporter), MILA - Quebec Artificial Intelligence Institute and Vector Institute.

Any further comments and implementation documentation.

No answer provided

Section 5 – Content Authentication & Provenance Mechanisms

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

- User disclosure (e.g., text notice, verbal statement, or system label)
- Distinct branding or labeling for AI-generated content (e.g., “AI-generated” tag, metadata label)
- Documentation or FAQs explaining when and how AI is used in the system

Provide any additional details or context on how or when users are informed they are interacting with advanced AI systems (e.g. if such mechanisms are planned, in testing, or applied only to certain products).

No answer provided

27. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems?

Not applicable

Any further comments and implementation documentation.

No answer provided

Section 6 – Research & Investment to Advance AI Safety & Mitigate Societal Risks

28. Does your organization advance research and investment in the following areas?

- Security
- Safety
- Data quality and representativeness
- Information integrity
- System performance and outcomes (e.g. accuracy, consistency)
- Explainability or interpretability
- Transparency
- Robustness or reliability

If yes, please describe key research or investment initiatives in the areas selected above (e.g., dedicated safety teams, funding of research programs, contributions to open-source safety tools, publishing research, partnerships and collaborative research initiatives). You may also indicate whether related outputs are publicly shared, shared with partners or within consortia or not publicly disclosed.

Research Reports and White Papers

TELUS Annual AI Reports (2024, 2025, 2026): 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 annual AI reports share the views from thousands of people on AI - their concerns, hopes and opinions about where this powerful technology should be headed. These reports are available to the public at:

<https://www.telus.com/ResponsibleAI>.

TELUS Digital GenAI Safety Model Benchmark: This study tested 34 AI models from 10 global providers across 620,000+ adversarial attack simulations. The full report is publicly available at <https://www.telusdigital.com/insights/fuel-ix/resource/genai-safety-benchmark-2026> and includes detailed vulnerability rates, model rankings, and analysis of safety factors.

NIST AI 800-4: Challenges to the Monitoring of Deployed AI Systems (2026) – TELUS contributed to this collaborative report published by the Center for AI Standards and Innovation (CAISI) in partnership with NIST.

<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-4.pdf>

Peer-Reviewed Publications and Conference Presentations

"Sustainable Involvement of Indigenous Peoples in AI" – Presented at the IEEE International Humanitarian Technology Conference (IHTC 2025). TELUS shared research insights on embedding Indigenous perspectives into AI development and governance. [DOI: 10.1109/IHTC65087.2025.11216330](https://doi.org/10.1109/IHTC65087.2025.11216330)

"Beyond the 'Universal User': AI Adoption and Literacy Patterns in Canada" – Presented at the Human-Computer Interaction International Conference (HCII 2026, Montreal). The findings demonstrate that self-reported usage and understanding deviate from traditional institutional expectations and suggest that AI education should employ diverse approaches to engage various stakeholders. https://doi.org/10.1007/978-3-032-29583-5_27

"From Principles to Practice: Translating Human-AI Interaction Research into Effective Human-Centred AI Product Design - Findings from a Cross-Industry Literature Review" – Presented at the Human-Computer Interaction International Conference (HCII 2026, Montreal). This research synthesizes human-AI interaction research into practical guidance for product design. https://doi.org/10.1007/978-3-032-30846-7_1

"Acceleration AI ethics and the Telus GenAI conversational agent" – Published in Law, Ethics & Technology (2026). TELUS' GenAI conversational agent was featured as a case study in this peer-reviewed journal article, written by an academic philosopher examining acceleration ethics and responsible AI implementation.

<https://doi.org/10.55092/let20260006>.

Collaborative Infrastructure and Standards Development

AI Consortium – TELUS co-founded the AI Consortium with Lightworks, Scotiabank, and Sun Life to build critical AI control infrastructure in Canada. The Consortium enables members to pool hands-on engineering, conduct deep research and align interests to jointly build and govern mission-critical AI control systems and intellectual property they would otherwise develop independently, with resulting IP deployed individually and available to members through perpetual-use and ownership rights. See: <https://www.telus.com/en/about/news-and-events/media-releases/Lightworks-Scotiabank-Sun-Life-and-TELUS-launch-AI-Consortium-to-jointly-build-critical-AI-control-infrastructure-in-Canada>

29. Does your organization pursue research or investment related to socio-economic or environmental considerations in the development and deployment of AI?

- Socio-economic considerations (e.g., AI adoption and productivity, workforce transitions, skills development, access to AI tools)
- Environmental considerations (e.g., energy use, computational efficiency, resource use)

If yes, please provide examples of relevant research or investment initiatives for the areas selected above.

TELUS has developed a Sovereign AI Factory in Rimouski, Quebec, powered by 99% renewable energy from Hydro Quebec and featuring intelligent cooling to deliver AI as a Service (AIaaS). Named Canada's fastest and most powerful supercomputer on the global Top500 list, this data centre is home to NVIDIA's advanced GPUs. The facilities are LEED Gold certified and rely on natural cooling, cutting water consumption by more than 75% compared to traditional data centres. With these credentials in place, TELUS' Sovereign AI Factory is among the most sustainable AI-ready data centres in the world.

TELUS collaborated with the Vector Institute on research for 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. Pilot testing showed a decrease of approximately 20% electricity consumption in hot summer months. TELUS has open-sourced the reference implementation for others to explore and apply in their own settings.

In 2025, TELUS launched the AI for Good program. The program partners with not-for-profit organizations to provide discounted or free access to TELUS' enterprise AI platform and Sovereign AI compute. Through AI for Good, TELUS partnered with Indigenomics to accelerate the development of IndigenomicsAI, an economic intelligence platform built within TELUS' Sovereign AI Factory to advance Indigenous economic growth and self-determination, for example.

Any further comments and implementation documentation.

No answer provided

Section 7 – Advancing Human and Global Interests

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

Yes

If yes, describe any digital literacy or training initiatives your organization supports (e.g., user education, public AI-education programs, school or university partnerships, community workshops). You may also indicate whether these efforts include or prioritise underserved or underrepresented communities.

With the rapid evolution of technology and the rise of AI we believe education in AI is critical for transparency. TELUS has implemented a comprehensive suite of digital literacy and education initiatives to improve user awareness and help people understand the nature, capabilities, and limitations of advanced AI systems.

Public AI Education Programs and Partnerships

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 provides free training on digital safety and includes a workshop on responsible AI to aid youth in navigating AI responsibly. See: <https://www.telus.com/Wise> and <https://cifar.ca/ai/destinationai/>

TELUS also partners with the University of Toronto on the Algorithmic Bias in Canada (ABC) project, an interdisciplinary initiative that aims to shape more equitable AI systems through academic collaboration, public engagement, and partnerships with industry, government, and Indigenous communities. A key component of this mission is raising public awareness about community-specific risks of algorithmic bias.

TELUS extends AI literacy beyond our organization through workshops and public engagement at major global forums, tailoring our message to diverse audiences. These workshops range from venues like the UN stage in Geneva to high school classrooms to innovation spaces like South by Southwest—tailoring our message to policymakers, youth, technologists, and civil society to ensure diverse voices are able to engage in and understand responsible AI. As a member of the International Telecommunication Union's AI Skills Coalition, TELUS shares knowledge on responsible AI development and inclusive governance.

Workforce AI Literacy

Internally, TELUS has developed an enterprise Data & AI Literacy program (introduced in 2021) that encourages team members to raise their skill level in working with data and AI through curated learning paths. This program is demonstrably advancing workforce capability, with employee confidence in their AI knowledge rising by 21 percentage points between 2024 and 2026, and the ability to explain AI's benefits and limitations increasing by 23 percentage points. TELUS has also been featured in the Business at OECD report as a leader in workforce AI literacy, underscoring our commitment to building AI competency across our organization and the broader Canadian workforce. See:

<https://www.businessatoecd.org/hubfs/website/documents/pdf/Education/Boosting%20Productivity%20and%20Business%20Growth%20The%20Role%20of%20AI%20Skills.pdf?hsLang=en>

31. Does your organization pursue AI projects that aim to deliver societal or public benefits, including through partnerships with civil society and community groups?

Yes

If yes, please provide examples, including any collaborations with civil society, community groups, or efforts to address broader societal challenges.

TELUS pursues AI projects designed to deliver significant societal and public benefits through our comprehensive AI for Good program, which advances the responsible adoption of AI through four key pillars: Applied AI in Action, Value Driven Research, Literacy and Skills Development, and Giving Back and Community Impact. See: telus.com/AIforGood

Applied AI in Action

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>

Value-Driven Research

TELUS believes diverse voices should shape AI's future. We publish annual research which reflects the hopes, concerns, and opinions of Canadians and Americans on AI. Our latest report, the 2026 AI Trust Atlas, captures perspectives from more than 11,000 Canadians and Americans. Special attention is given to historically underrepresented communities as defined by the Government of Canada, including boosted samples for underrepresented groups including Indigenous Peoples, Black women, LGBTQ2S+ individuals, people with disabilities, low-income individuals, seniors, and recent immigrants to ensure diverse perspectives were represented. highlighting the importance of including a wide range of voices to build trustworthy AI. See: telus.com/ResponsibleAI

Literacy and Skills Development

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 and includes a new workshop on responsible AI to aid youth in navigating AI responsibly.

See: <https://www.telus.com/Wise> and <https://cifar.ca/ai/destinationai/>

Giving Back and Community Impact

TELUS is committed to making AI capabilities accessible to organizations creating positive change. Through our AI for Good program, we provide discounted or free access to Fuel iX and the Sovereign AI Factory to not-for-profits and community organizations. For example, we partnered with Indigenomics to launch IndigenomicsAI, an economic intelligence platform that leverages TELUS' Sovereign AI Factory to advance Indigenous economic growth and economic self-determination. See: <https://www.telus.com/en/about/news-and-events/media-releases/TELUS-and-Indigenomics-partner-to-advance-Indigenous-economic-outcomes-using-sovereign-AI>

TELUS also partnered with Indigenous AI start up wâsikan kisewâtisiwin to become its first beta tester, integrating their Indigenous-informed writing tool into the TELUS Sovereign AI Factory. See:

[https://www.wasikankisewatisiwin.ca/news/kind-electricity?
_sm_ows=QWDWDqMvkfj0sq50vnq0F1W40VRvSvnqMVVVVVVVV](https://www.wasikankisewatisiwin.ca/news/kind-electricity?_sm_ows=QWDWDqMvkfj0sq50vnq0F1W40VRvSvnqMVVVVVVVV)

Any further comments and implementation documentation.

No answer provided