



TELUS Supplier Code of Conduct

Last updated November 24, 2025



Introduction

We value our supplier relationships as essential partnerships in achieving our business objectives and organizational success. We prioritize suppliers who demonstrate a strong commitment to sustainable development through ethical business practices, robust labor standards, comprehensive health and safety protocols, environmental stewardship, and full regulatory compliance, ensuring the well-being of their employees, contractors, and communities.

This Supplier Code of Conduct (the Code) is consistent with the TELUS Code of Ethics and Conduct that applies to our employees and contractors. Built on internationally recognized standards of ethical business conduct, this Code applies to all TELUS suppliers. Our suppliers must comply with both this Code and all applicable laws and regulations in their operating jurisdictions. Where discrepancies exist between this Code and local laws or regulations, suppliers must adhere to the stricter requirements.

This Code extends beyond legal compliance. It draws upon internationally recognized standards to advance social and environmental responsibility and business ethics, reflecting TELUS' commitment to leading corporate citizenship.

Suppliers must meet or exceed the requirements set forth in this Code and cause their, and their affiliates', suppliers, employees and contractors to perform obligations to TELUS in a manner consistent with the standards set out in this Code. TELUS reserves the right to periodically review and update this Code.

For clarity, the obligations set out in this Code are in addition to, and do not limit, suppliers' obligations under any agreements with TELUS.

A - Ethics

To meet social responsibilities and achieve long-term success in the marketplace, our suppliers must uphold high ethical standards, including:

- 1) **Business Integrity:** Suppliers must maintain the highest standards of courtesy, professionalism, ethics, and honesty in all interactions with customers, shareholders, suppliers, employees, governments, and communities. Suppliers must comply with all applicable federal, provincial, state, and local laws.
- 2) **Anti-Bribery & Anti-Corruption:** Suppliers must comply with all applicable anti-bribery and corruption laws and the TELUS Anti-Bribery & Corruption Policy. They must refrain from engaging in bribery, corruption, kickbacks, extortion, or any conduct that could be viewed as an attempt to improperly influence business decisions or create a sense of obligation. This includes the promising, offering, approving, giving, or accepting of payments or gifts for such purposes. TELUS



prohibits facilitation payments, even if they are not illegal in a particular jurisdiction. Facilitation payments are small, unofficial payments made to secure or expedite routine government actions, such as processing permits or providing routine police protection.

- 3) **Gifts & Gratuities:** Suppliers must familiarize themselves with the TELUS Code of Ethics and Conduct, which provides guidance to TELUS team members on offering or accepting gifts, gratuities, rewards, favours, or benefits—particularly for those in selection, negotiation, purchasing, or contract management roles. Suppliers must not place TELUS team members in positions where they are, or may be perceived to be, in breach of the TELUS Code of Ethics and Conduct.
- 4) **Privacy:** Suppliers must respect the privacy of TELUS customers and team members and demonstrate accountability for all personal information entrusted to them, including information collected or created on TELUS' behalf. Suppliers must collect, use, and disclose personal information only as directed by TELUS or as required by law. Suppliers must assist TELUS in meeting privacy obligations under applicable laws, contracts, and TELUS' privacy standards. This includes facilitating access requests and fulfilling individual rights, informing TELUS of actual or suspected data breaches, supporting TELUS' responses to inquiries, complaints, and investigations, and implementing effective retention processes. Suppliers must take all reasonable steps to support TELUS in upholding the TELUS Privacy Commitment, the Privacy Information page for TELUS Business Customers, and similar applicable policies.
- 5) **Information Security & Cybersecurity:** Suppliers must appropriately safeguard all TELUS information entrusted to them, and maintain the highest level of cybersecurity in their own operations and activities as well as those of any subcontractors or suppliers. Unless disclosure is authorized or legally mandated (for example, by court order), our suppliers must protect confidential and restricted information, in compliance with all applicable laws and contractual obligations. Suppliers must protect TELUS' information and operations by working with their designated TELUS business prime to obtain and comply with applicable TELUS security policies and controls. Suppliers must not bypass, circumvent, or otherwise compromise TELUS' security policies and controls. Should a supplier become aware of a cyber incident or potential breach that could impact TELUS or the security of TELUS' operations or data, such supplier must immediately report it to their TELUS business prime and, if requested, provide a detailed written report, including any potential impacts on TELUS data or systems.
- 6) **Intellectual Property:** Suppliers must respect the intellectual property rights of TELUS and others, and comply with their contractual and other obligations pertaining to intellectual property rights.
- 7) **Fair Business, Advertising & Competition:** Suppliers must adhere to fair business practices and comply with all applicable laws relating to marketing, anti-spam, advertising, and competition standards in the jurisdictions where they operate.
- 8) **Conflicts of Interest:** Suppliers may have business relationships beyond TELUS. These relationships must not, and must not reasonably appear to, compromise suppliers' relationship



with TELUS or suppliers' ability to make impartial and objective business decisions in connection with the supply of goods and/or services to TELUS.

- 9) **TELUS Property:** Suppliers must implement reasonable technological, administrative, and physical safeguards to protect all TELUS property in their possession or control. This includes TELUS proprietary, confidential, and restricted information, facilities, equipment, vehicles, funds, communication networks, information systems, and access controls such as passwords, identification keys, cards, and hand-held user authentication devices.
- 10) **Artificial intelligence:** Suppliers must ensure the ethical use of Artificial Intelligence (AI) through responsible, appropriate, and accountable practices across all phases of AI development, usage and provisioning. This requires adherence to principles promoting human rights, fairness, diversity, equality, transparency, safety, and security, with AI designed using a human-in-control approach. Suppliers must comply with all applicable laws and regulations governing AI technologies and implement adequate controls to ensure compliance across their operations and sub-tier suppliers, in alignment with the [TELUS Trust Model](#) and [TELUS Approach to Responsible AI](#). Suppliers must not use TELUS' data for AI training unless expressly permitted, must disclose to TELUS its use of AI in relevant product or service, and must provide TELUS with any reasonably requested information and support to enable TELUS to comply with its own obligations under applicable laws and regulations. All AI solutions must be explainable, transparent, and free from unintended harms and bias, and suppliers are responsible for demonstrating how these principles are embedded in their AI practices and solutions.
- 11) **Non-Retaliation:** Suppliers must not retaliate against anyone who files a report or complaint in good faith relating to the supplier or a violation of this Code, whether reported internally (such as through a whistleblower mechanism), to TELUS, or to any government agency. Suppliers must maintain whistleblower confidentiality.

B - Labour

Our suppliers must uphold the human rights of workers, and treat them with dignity and respect in compliance with internationally accepted laws and standards governing working conditions, such as the core conventions of the International Labour Organization (ILO) and the United Nations Guiding Principles on Business and Human Rights. All workers must be legally entitled to work in the country in which they live, and must be granted the protections and rights granted to legal workers in that country. These requirements apply to all workers including temporary, migrant, student, contract, direct employees, apprenticeship program participants, and any other type of worker. Suppliers must take appropriate actions against any violations of the labour standards expressed in this Code:

- 1) **Freely Chosen Employment:** Suppliers must ensure that all work being performed on behalf of our suppliers is voluntary, and workers are free to leave at any time or terminate their employment.



Forced, bonded (including debt bondage) or indentured labour, involuntary prison labour, slavery or trafficking of persons must not be used. This includes transporting, harbouring, recruiting, transferring or receiving vulnerable persons by means of threat, force, coercion, abduction or fraud for the purpose of exploitation. While workers may be asked to provide government-issued documentation as identification, they must not be required to surrender government-issued identification, passports or work permits as a condition of employment.

- 2) **Child Labour:** Suppliers must not use child labour in any part of their business operations. The minimum age for employment or work must be 15 years of age (or 14 where the laws of the country permit) or the age for completing compulsory education in that country, whichever is higher. If child labour is detected, the supplier must immediately cease such employment and take corrective action to prevent future violations
- 3) **Working Hours:** Suppliers must ensure that work weeks do not exceed the maximum number of hours set by local law. Where no applicable laws exist, suppliers must not require work exceeding 60 hours per week, including overtime, or more than six consecutive days without a rest day, except in emergency or unusual situations.
- 4) **Wages & Benefits:** Compensation paid to workers must comply with all applicable wage laws, including those relating to minimum wages, overtime hours, and legally mandated benefits. Where no wage laws exist, workers must be paid at least the minimum local industry standard. Deductions from wages as a disciplinary measure are not permitted. Suppliers must provide workers with timely documentation of their compensation basis, such as pay stubs or similar records.
- 5) **Non-Discrimination:** Suppliers must maintain a work environment, and recruitment practices (screening, hiring and retaining) free of harassment and discrimination and must not engage in discrimination based on race, national or ethnic origin, religion, age, sex, gender identity or expression, sexual orientation, marital status, family status, genetic characteristics, disability, or conviction for which a pardon has been granted or in respect of which a record suspension has been ordered.
- 6) **Freedom of Association & Collective Bargaining:** Suppliers must respect the rights of workers to freely join labour unions, seek representation and join workers' councils, and to bargain collectively in accordance with local laws. Suppliers must enable workers and their representatives to openly communicate and share ideas and concerns with our suppliers' management regarding working conditions and management practices without fear of discrimination, reprisal, intimidation or harassment.
- 7) **Legal Eligibility to Work:** Suppliers must ensure that all foreign workers performing work on behalf of TELUS or at TELUS offices, facilities, or customer premises have the appropriate work permits and comply with all local immigration laws and regulations.



C - Health & Safety

Suppliers must comply with all applicable health and safety laws and ensure all services are performed with appropriate health and safety diligence. Where appropriate, suppliers must develop, implement, and provide worker training on policies, programs, and procedures addressing the following health and safety matters:

- 1) **Occupational Health & Safety:** Suppliers must control exposure to health and safety hazards through proper design, engineering and administrative controls, preventative maintenance, and safe work procedures. Where hazards cannot be adequately controlled, workers and other persons at or near worksites must be provided with appropriate and well-maintained personal protective equipment. Health hazards include exposure to chemical, biological, and physical agents. Safety hazards include inadequate guards and barriers around machinery. Suppliers must not take disciplinary action against workers who raise legitimate health and safety concerns.
- 2) **Property Risk Reduction & Emergency Preparedness:** Suppliers must identify and mitigate property and life safety risks, including structural integrity of facilities, fire risk, flooding risk, power supply continuity risk, and other risks that could impact worker lives and well-being, service delivery to TELUS, or TELUS operations. Suppliers must identify and assess potential emergency situations and minimize their impact by implementing comprehensive emergency plans and response procedures. These must include emergency reporting, notification and evacuation procedures, worker training and drills, appropriate fire detection and suppression equipment, adequate exit facilities, and recovery plans.
- 3) **Occupational Injury & Illness:** Suppliers must have procedures and systems in place to manage, track and report occupational injury and illness, including provisions to:
 - a) encourage reporting
 - b) classify and record injury and illness cases
 - c) provide necessary medical treatment
 - d) investigate cases and implement corrective actions to eliminate their causes
 - e) facilitate the return of workers to work.
- 4) **Fit for Work:** Suppliers must require workers to report to work fit for duty, with their ability to work safely not impaired by any substance or condition. Workers must be free from the impairing effects of alcohol, drugs, medications, or any other substance that could compromise workplace safety.



D - Environmental Responsibility

TELUS is committed to protecting our planet, with science-based targets to reduce Scope 1, 2, and 3 greenhouse gas (GHG) emissions and the goal to achieve net zero emissions by 2040. Suppliers must support these environmental objectives.

Suppliers must comply with the [TELUS Environmental Policy](#), [TELUS Sustainability Paper & Packaging Policy](#) and all applicable environmental laws, regulations, and standards. TELUS maintains an ISO 14001-certified Environmental Management System (EMS). Suppliers are expected to implement comparable environmental strategies, including policies and programs to identify, manage, monitor, report, and continuously reduce environmental impacts from their operations, including but not limited to:

- 1) **Resource use & pollution:** Suppliers must optimize consumption of natural resources and implement processes that drive technological advancements for resource optimization. This includes efficient use of fossil fuels, water, forest products, and other raw materials, while minimizing negative impacts on biodiversity, ecosystems, and habitats.
- 2) **Hazardous substances:** Dangerous goods, chemicals and other substances or materials posing a hazard to humans or the environment must be identified, labeled and managed to ensure their safe handling, movement, storage, use, recycling or reuse and disposal in accordance with local, provincial and/or federal regulations.
- 3) **Waste management and circular economy:** Suppliers must implement a systematic approach to identify, manage, reduce, and responsibly dispose of all types of waste. Suppliers must make efforts to implement and allow TELUS to implement circular economy strategies related to the lifecycle impacts of products and services, from sourcing and production through use, recycling, refurbishment and resale.
- 4) **GHG emissions & energy consumption:** Suppliers must actively monitor, report, and set science-aligned targets to reduce GHG emissions and energy consumption from their operations and value chain. Suppliers must provide data on GHG emissions and progress toward reduction targets to TELUS upon request.
- 5) **Responsible Sourcing of Materials:** Suppliers must evaluate the origin or source of their materials throughout their supply chains to reasonably ensure that they have not been obtained in an illegal or unethical manner and are in compliance with [TELUS' Sustainable Paper & Packaging Policy](#).
- 6) **Conflict Minerals:** Where applicable, our suppliers must have a policy regarding conflict minerals to reasonably ensure that the tantalum, tin, tungsten, gold and/or other rare earth minerals in their products do not directly or indirectly finance or benefit groups that are perpetrators of human



rights abuses. Relevant suppliers must exercise due diligence on the source and chain of custody of these minerals and make their due diligence measures available to TELUS upon request.

E - Social Responsibility

- 1) **Supplier Diversity & Indigenous Procurement:** TELUS' supplier diversity and Indigenous procurement program takes active measures to provide access to a supply base that reflects the diversity of where we live, work and serve by encouraging economic development for culturally diverse organizations. TELUS recognizes that meaningful Indigenous Economic Development is essential to economic reconciliation in Canada. Through our Indigenous procurement program, we aim to remove barriers, create opportunities, and support the growth of Indigenous businesses across our supply chain. We encourage our suppliers to join us by developing Indigenous procurement strategies and forming meaningful partnerships. Our suppliers must:
 - a) Make a reasonable effort to continuously identify and partner with diverse and Indigenous suppliers,
 - b) Implement, or expand and increase, their own supplier diversity program,
 - c) Disclose supplier diversity program goals, plans and spend to TELUS on a semi-annual basis, and report progress every quarter against the targets agreed upon between supplier and TELUS, and
 - d) Give notice to TELUS in case of any changes to such a diversity program.
- 2) **Community Investment:** Suppliers are encouraged to meaningfully engage and invest in the communities in which they live, work and serve to foster social and economic development.
- 3) **Accessibility:** Suppliers must recognize that access and usability of products, services, solutions, and environments by persons of all abilities is integral to being a leading service provider and promoting accessibility and inclusion within our workplace and the communities we serve. Suppliers must incorporate universal and accessible design principles to remove existing barriers and avoid introducing new barriers that may impede a person from independently experiencing and using products, services, solutions, or environments. This includes consulting with persons with disabilities throughout the design process.

F - Management System

Suppliers are expected to have in place the appropriate management system to ensure

- (a) compliance with applicable laws and regulatory requirements in the jurisdiction in which they operate, and customer requirements related to the supplier's operations and products;
- (b) conformance with the principles of this Code; and



(c) identification and mitigation of operational risks related to this Code. The management system must facilitate continuous improvement. TELUS recognizes that management system design must be appropriately scaled to the particulars of each supplier's business.

The suppliers' management systems must include the following elements:

- 1) **Management Accountability & Responsibility:** Clearly identified supplier representative responsible for ensuring implementation of the management systems and associated programs.
- 2) **Legal & Customer Requirements:** Suppliers must establish and maintain processes to identify, monitor, and understand all applicable laws and regulatory requirements in the jurisdictions where they operate, as well as customer contractual requirements, including business continuity planning and operational resilience capabilities.
- 3) **Risk Assessment & Risk Management:** Suppliers must have processes to identify environmental, health and safety, labour practice, privacy, and fraud risks associated with their operations and affecting customers' information and proprietary rights. Suppliers must determine the relative significance of each risk and implement appropriate technical, procedural, and physical controls to manage identified risks and ensure regulatory compliance.
- 4) **Communication & Training:** Suppliers must establish processes to communicate clear and accurate information about their policies, procedures, and improvement objectives to workers, and implement training programs to ensure workers meet all applicable legal, regulatory, and customer contractual requirements.
- 5) **Compliance Assessments & Corrective Actions:** Suppliers must perform periodic self-evaluations to ensure conformity with all applicable legal and regulatory requirements, the requirements of this Code, and customer contractual obligations. Suppliers must maintain processes to ensure timely correction of any identified deficiencies.
- 6) **Accurate Accounts & Record Keeping:** Suppliers must create and maintain accurate and reliable financial and business records to ensure legal and regulatory compliance, meet supplier requirements, protect confidential information and privacy, and communicate accurate information to customers. All business dealings must be accurately reflected in business records, and all records relating to contractual supply arrangements must be protected and retained in accordance with applicable legal obligations and compliance requirements.

G - Implementation & Compliance

Suppliers must ensure their employees and contractors working on TELUS' projects understand and comply with the contents of this Code.



TELUS is committed to continuous improvement and encourages suppliers to proactively share suggestions in regards to this Code, business processes and performance, and relationship improvement. Suppliers are expected to proactively seek opportunities for continuous improvement throughout their own operations.

Suppliers must monitor compliance with the terms of this Code throughout their own operations as well as any Related Parties' operations. Suppliers are obligated to immediately disclose any known or suspected violations of the Code to their TELUS representatives or Ethics Point (contact below).

While adherence to the requirements in this Code are the responsibility of the Supplier, TELUS may verify Supplier compliance with the Code through a variety of tools, including but not limited to:

- a) Suppliers' self-evaluations;
- b) Ongoing improvement programs; and
- c) On-site inspections or audits by TELUS or a representative designated by TELUS.

It is important that non-compliant and unethical matters are reported. We encourage anyone who knows of or suspects violations or potential violations of laws and regulations, this Code, or TELUS policies, standards, procedures, and other requirements shared with suppliers to report through the following channels:

- a) 1-888-265-4112 or
- b) www.telus.ethicspoint.com

TELUS is committed to fair and appropriate treatment and respects the confidentiality of all parties involved. Reports may be made anonymously. The privacy of reporters will be respected, and confidential information will be shared only on a need-to-know basis or as required by law. TELUS prohibits retaliation or reprisal against suppliers and their workers who report concerns in good faith.

Links & Information

- **TELUS website:** www.telus.com
- **TELUS Data and Trust Office:** Datatrustoffice@telus.com
- **TELUS Data management standards contact:** SecurityGRA@telus.com
- **TELUS Sustainability Report:** <https://telus.com/sustainability>