Teradata

Third-Party Code of Conduct

Version 2.0 | Effective July 2026 | Annual review: July 2027
Questions: supplier.onboarding@teradata.com | Ethics Helpline: +1-866-455-0993

A note from our VP of Sourcing and Procurement- Carrie Adank

At Teradata, our commitment to responsible business extends beyond our own operations to every partner, vendor, and supplier that helps us deliver for our customers. This Third-Party Code of Conduct sets out the standards we expect all third parties to uphold — standards rooted in ethics, respect for people, and care for the environment.

We recognize that building ethical partnerships is a shared journey. Teradata is committed to supporting its partners in meeting these standards, and we ask that you engage with this Code in the spirit of continuous improvement and transparency. Where local law requires higher standards than this Code, local law prevails. Where this Code is more rigorous, the Code applies.

Questions about this Code should be directed to supplier.onboarding@teradata.com.

Scope and Application

This Third-Party Code of Conduct (the **"Code"**) applies to all entities and individuals providing goods or services to Teradata Corporation or any of its subsidiaries, including distributors, resellers, marketing representatives, vendors, service providers, consultants, contractors, and staffing agencies (collectively, **"Third Parties"**).

This Code is intended to supplement and reinforce the principles set forth in the Teradata Code of Conduct by establishing specific expectations for Third Parties.

Third Parties are responsible for ensuring that their workers — including employees, temporary staff, agents, and contractors — and any sub-contracted party performing work on behalf of Teradata, are informed of and agree to comply with this Code.

Any violation of this Code may result in remedial action up to and including suspension or termination of the business relationship with Teradata. Where appropriate and feasible, Teradata will work constructively with Third Parties to address identified issues through a corrective action process before exercising termination rights.

Teradata recognizes that not all provisions of this Code are equally relevant to all Third Parties. Requirements should be proportionate to the nature, scale, and risk profile of the third-party relationship.

While this Code sets forth the Company's expectations for Third Parties, it does not supersede any binding contractual obligations. In the event of any inconsistency, conflict, or discrepancy

between this Code of Conduct and a written agreement between the Third Party and the Company, the written agreement shall control.

1. Ethics and Governance

1.1 Anti-Bribery and Anti-Corruption

Third Parties shall maintain a zero-tolerance policy that forbids any form of bribery, corruption, kickbacks, extortion, and embezzlement. All business dealings must be transparent and conducted with integrity.

As outlined in Teradata's Global Anti-Corruption Policy, all Third Parties must comply with all applicable anti-bribery, anti-corruption, anti-money-laundering, anti-fraud, antitrust/competition, and import/export compliance laws in every jurisdiction where Teradata conducts business, including the United States Foreign Corrupt Practices Act (FCPA), the United Kingdom's Bribery Act and other applicable local laws. Third Parties acting on Teradata's behalf cannot take actions that Teradata could not take itself in this regard.

Translations of Teradata's Anti-Bribery Policy are available at "Additional Resources" on the Teradata Code of Conduct webpage.

Specifically, Third Parties must not:

- Offer, pay, promise, authorize, request, or accept any bribe, kickback, improper payment, or improper advantage, whether directly or indirectly through another party;
- Offer or provide anything of value to any person, including government officials, government-related entities, customers, prospective customers, business partners, or Teradata employees, for the purpose of improperly influencing a decision, obtaining or retaining business, securing an improper advantage, or causing someone to misuse their position;
- Provide gifts, entertainment, hospitality, travel, employment opportunities, subcontracting opportunities, charitable contributions, sponsorships, political contributions, or other benefits on Teradata's behalf in a manner intended to improperly influence a business decision or circumvent Teradata's policies;
- Provide gifts or entertainment to Teradata employees to obtain or retain business or gain any improper business advantage; or
- Provide gifts or entertainment to customers, prospective customers, or other third parties on Teradata's behalf unless the business courtesy is lawful, modest, infrequent, transparent, accurately recorded, consistent with the recipient's policies, and permitted under Teradata's applicable policies.

Teradata prohibits all facilitating payments (sometimes referred to as 'grease payments'), regardless of whether they are permitted under local law or custom. Third Parties must not make facilitating payments on Teradata's behalf and must immediately report any request or solicitation for a facilitating payment to Teradata's Ethics & Compliance Team at E&C@teradata.com. In addition, gifts and entertainment to Teradata employees or on Teradata's behalf to third parties (e.g. customers and prospective customers) must not exceed the dollar values listed in Teradata's Code of Conduct.

Cash and cash equivalents, including gift cards, vouchers, prepaid cards, loans, or other cash-like benefits, are prohibited in all circumstances when provided on Teradata's behalf.

All gifts, entertainment, hospitality, travel, or other things of value involving government officials or government-related entities on Teradata's behalf must be reviewed and pre-approved by Teradata's Ethics & Compliance Team before any commitment is made. Some Teradata customers, prospective customers, partners, or other third parties may be owned in whole or in part by a governmental entity, state-owned enterprise, public institution, or similar organization. As a result, their representatives may be considered government officials or otherwise present heightened anti-bribery and anti-corruption risk.

Third Parties must promptly disclose and report any actual or suspected bribery, kickback, facilitating payment request, improper gift or entertainment request, conflict of interest, request to hire or retain a customer's relative or associate, or other conduct that may violate this Code, Teradata's policies, or applicable law. Third Parties must also respond timely and accurately to Teradata's questions and requests related to third-party due diligence, monitoring, audits, certifications, and compliance reviews.

1.2 Fair Competition and Antitrust

Third Parties must comply with all applicable competition and antitrust laws wherever they conduct business. Third Parties must compete fairly and must not enter into any agreement, understanding, coordination, or arrangement — whether formal or informal, written or unwritten — that could improperly restrict competition.

Third Parties must not:

- Engage in price-fixing, bid rigging, market allocation, customer allocation, output restrictions, group boycotts, or other practices that unlawfully restrict competition;
- Exchange, request, receive, or disclose competitively sensitive information with competitors, including pricing, discounts, costs, margins, bids, customers, sales strategy, product plans, territories, or marketing strategy;
- Use Teradata confidential information or competitively sensitive information to benefit a competitor or improperly restrict competition; or
- Participate in any discussion or conduct that could create the appearance of improper coordination with competitors.

When attending industry associations, standard-setting organizations, conferences, trade shows, benchmarking activities, or similar forums, Third Parties must avoid discussions involving pricing, bids, customers, markets, territories, business strategy, or any other topic that could constitute antitrust.

Third Parties must maintain appropriate information barriers when supporting Teradata while also working with competitors, customers, suppliers, or other market participants.

1.3 Conflicts of Interest

Third Parties must avoid actual, potential, or perceived conflicts of interest when conducting business with or on behalf of Teradata. Third Parties must promptly disclose any relationship, financial interest, outside activity, or other circumstance that could create — or appear to create — a conflict of interest with Teradata business decisions.

Conflicts of interest may include personal, family, financial, employment, consulting, ownership, referral, or other business relationships with Teradata employees, customers, suppliers, resellers, distributors, government officials, or other relevant decision-makers.

Disclosures should be made to E&C@teradata.com. Third Parties must cooperate with Teradata's review of disclosed conflicts and follow any required mitigation steps.

1.4 Import / Export Controls and Trade Sanctions

Third Parties must comply with all applicable import and export control laws, trade sanctions regimes, and anti-boycott regulations in all jurisdictions where they operate, including regulations administered by the US Department of Commerce (BIS), the US Department of Treasury (OFAC), and equivalent authorities in other jurisdictions. Third Parties must not facilitate transactions involving sanctioned countries, entities, or individuals.

To meet these obligations, Third Parties are expected to maintain a program that at least includes the following activities:

- **Screen and verify parties**: Conduct appropriate and ongoing screening of customers, business partners, subcontractors, and transactions against applicable government restricted party lists.
- **Implement controls and procedures**: Maintain documented internal controls, policies, and procedures designed to ensure compliance with trade laws and regulations, including export classifications and licensing requirements where applicable.
- **Obtain required authorizations**: Secure all necessary export, re-export, and import licenses or other governmental approvals prior to engaging in controlled activities.
- **Ensure accurate documentation**: Maintain complete, accurate, and auditable records of all transactions, classifications, licenses, and shipping documentation in accordance with applicable legal requirements.
- **Escalate and report risks**: Promptly notify Teradata of any actual or suspected violations, compliance concerns, or government inquiries related to trade controls.
- **Flow down requirements**: Ensure that subcontractors and downstream partners involved in Teradata-related work are informed of and comply with these trade compliance obligations.
- **Provide training and oversight**: Ensure relevant personnel receive appropriate training on trade compliance requirements and that oversight mechanisms are in place to monitor adherence.

Failure to meet these expectations may result in corrective action, including suspension or termination of the business relationship.

1.5 Accurate Records and Financial Integrity

Third Parties must maintain complete, accurate, and transparent books, records, and accounts that fairly reflect the true nature, value, and purpose of all transactions related to their work for Teradata.

Third Parties must not falsify, misrepresent, conceal, or omit information in any document, invoice, expense claim, business record, certification, or communication related to Teradata business. Undisclosed side agreements, off-book arrangements, false or misleading entries, inflated invoices, inaccurate descriptions of services, or records that disguise improper payments or benefits are prohibited.

Third Parties must ensure that all invoices and payment requests are supported by appropriate documentation and accurately reflect goods or services actually provided. Third Parties must cooperate with Teradata's due diligence, audit, monitoring, and records requests.

2. Data, Privacy and Cybersecurity

Teradata requires that data entrusted to its third parties is handled with the same care, security, and accountability it applies to its own systems. Third Parties must protect Teradata data, customer data, personal information, or confidential information in accordance with applicable laws, contractual obligations, Teradata policies, and industry-appropriate privacy and security practices.

2.1 Data Privacy

Third Parties must comply with all applicable privacy, data protection, and cross-border data transfer laws when processing personal information in connection with Teradata business, including employees, contractors, customers, and consumers. This includes, where applicable but not limited to:

- EU General Data Protection Regulation (GDPR)
- UK Data Protection Act
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Singapore Personal Data Protection Act (PDPA)
- China Personal Information Protection Law (PIPL)
- India Digital Personal Data Protection Act (DPDP Act)
- All other applicable national and regional data protection laws

Third Parties must support Teradata in meeting applicable privacy obligations, including requests related to access, correction, deletion, portability, restriction, opt-out, consent, or other individual privacy rights as may be applicable. Third Parties must promptly notify Teradata of any privacy inquiry, complaint, regulatory request, suspected unauthorized processing, or actual or suspected compromise of personal information.

For more information, see the Teradata Global Privacy Statement.

2.2 Cybersecurity

Third Parties that access, store, process, or transmit Teradata data or systems must maintain appropriate information security controls. At a minimum, Third Parties are expected to:

- Implement and maintain an information security management system aligned to ISO 27001 or an equivalent standard (e.g. SOC 2 Type II)
- Apply appropriate access controls, encryption, and incident response capabilities
- Conduct regular security assessments and vulnerability management
- Ensure that personnel with access to Teradata data receive appropriate security training

2.3 Confidentiality and Intellectual Property

Third Parties must protect Teradata's confidential information, trade secrets, and intellectual property. Confidential information may only be used for the authorized purpose for which it was disclosed and must be returned or securely destroyed at the end of the engagement. Third Parties must not obtain, distribute, or use unlicensed software or copyrighted material without proper authorization.

Third Parties who receive material non-public information about Teradata in the course of their engagement must not trade in Teradata securities on the basis of such information.

2.4 Ethical Use of Artificial Intelligence

Third Parties are expected to use AI tools in a manner that reflects Teradata's commitment to honesty, respect for rights, confidentiality and fairness. Third Parties utilizing artificial intelligence (AI) tools, including generative AI, in connection with any Teradata-related work must do so responsibly and in accordance with applicable laws, regulations, and Teradata policies.

Third Parties must:

- Disclose to Teradata the AI tools and systems used in performing Teradata-related services and clearly identify any work product or deliverable that is AI-generated or AI-assisted
- Not input Teradata confidential information, proprietary data, personal data, or intellectual property into any AI tool unless expressly authorized by Teradata in writing
- Ensure that AI-generated outputs are reviewed by qualified personnel for accuracy, quality, bias, and compliance before incorporation into any Teradata deliverable or decision
- Implement safeguards to prevent AI tools from producing discriminatory, misleading, or harmful outcomes, and maintain appropriate human oversight of AI-assisted processes
- Not use Teradata data to train, fine-tune, or improve any AI model without Teradata's prior written consent
- Ensure that their use of AI does not infringe upon the intellectual property rights of any third party

- Promptly notify Teradata of any material changes to AI systems used in Teradata-related work and cooperate with Teradata's right to audit AI practices and governance frameworks

3. Labor and Human Rights

Teradata is committed to respecting internationally recognized human rights in its own operations and throughout its third party relationships. This section is aligned with the ILO Core Conventions, the UN Guiding Principles on Business and Human Rights (UNGPs), and the OECD Guidelines for Multinational Enterprises. These standards apply to all Third Parties; specific provisions are noted where they apply primarily to manufacturing, facilities, or labor-intensive operations.

3.1 Freely Chosen Employment

Third Parties must not use or permit any form of forced, bonded, indentured, or compulsory labor. All work must be voluntary, and workers must be free to terminate their employment at any time without penalty, provided reasonable notice is given as agreed in their contract.

Specifically, Third Parties must not:

- Withhold workers' identity documents, passports, or work permits
- Restrict workers' freedom of movement within or between facilities
- Require workers to pay recruitment fees or other fees for their employment, directly or through third parties
- Use threats of violence, verbal or psychological harassment, or debt bondage to retain workers

3.2 Child Labor

Third Parties must not employ any person under the age of 15, under the age for completing compulsory education, or below the minimum legal working age in the relevant jurisdiction — whichever is highest (aligned to ILO Conventions 138 and 182). Third Parties must implement an appropriate mechanism to verify the age of workers. Young workers under 18 must not perform work that is hazardous, involves night shifts, or otherwise jeopardizes their health, safety, or education.

3.3 Fair Wages and Working Hours

Third Parties must pay workers on time and in full. Where a minimum wage is set by law, workers must be paid at least that amount. Where no legal minimum wage exists, workers must be paid at least the prevailing industry wage or a living wage benchmark, as required by local law, a collective agreement, or commonly accepted practice (whichever is higher). Overtime must be paid at the rate required by local law.

Working hours must not exceed 60 hours per week (including overtime), or the maximum set by local law, whichever is lower, except in verified emergency circumstances. Workers must receive

at least one rest day per seven days. Deductions from wages must not be used as a disciplinary measure.

3.4 Non-Discrimination and Equal Opportunity

Third Parties must provide equal opportunity in the workplace. No worker or job applicant may be discriminated against in hiring, compensation, promotion, or any other employment decision on the basis of race, ethnicity, national origin, religion, age, sex, gender identity or expression, sexual orientation, marital status, disability, pregnancy, political affiliation, union membership, veteran/military status, genetic information, or any other characteristic protected by applicable law.

Third Parties must maintain a workplace free from harassment, intimidation, bullying, and abuse of any kind.

3.5 Freedom of Association and Collective Bargaining

Third Parties must respect the right of workers to associate freely, form or join a labor union of their choosing, and bargain collectively in accordance with applicable law (ILO Conventions 87 and 98). Where local laws restrict these rights, Third Parties should permit workers to elect and join alternative lawful forms of worker representation. Workers must be able to communicate openly with management regarding working conditions without fear of reprisal.

3.6 Health and Safety

Third Parties must provide a safe and healthy working environment for all workers. Third Parties should align their occupational health and safety management to ISO 45001 or equivalent, and must:

- Identify and assess workplace hazards and implement appropriate controls
- Provide appropriate protective equipment at no cost to workers
- Ensure workers receive health and safety training relevant to their role
- Maintain records of workplace incidents and implement corrective actions
- Ensure emergency response plans are in place and communicated to all workers

These requirements apply with particular emphasis to Third Parties in hardware, manufacturing, facilities, and logistics categories.

Third-party personnel working on Teradata premises or attending Teradata-sponsored events must comply with Teradata's drug-free workplace standards. The use, possession, or distribution of illegal substances on Teradata premises is strictly prohibited.

3.7 Worker Grievance Mechanisms

Third Parties must maintain accessible and confidential grievance channels that allow their workers to raise concerns about working conditions, labor rights violations, or other workplace issues without fear of retaliation. These channels must be separate from the Teradata Ethics Helpline, which is used to report concerns about Teradata’s Code and standards.

3.8 Modern Slavery and Human Trafficking

Teradata is committed to conducting business ethically and with integrity, and to implementing and enforcing effective systems and controls to ensure that modern slavery and human trafficking are not taking place within our business operations or with our third parties or partners.

We expect all third parties—including suppliers, contractors, consultants, and business partners ("Third Parties")—to share and uphold this commitment. Third Parties must cooperate with any Teradata request related to verifying compliance with this commitment.

4. Environment and Climate

Teradata is committed to reducing its environmental footprint and expects Third Parties to do the same. This section is aligned with GRI Standards (305, 306) and Teradata's obligations under CSRD and CDP value chain reporting requirements.

4.1 Environmental Compliance

Third Parties must comply with all applicable environmental laws and regulations in every jurisdiction where they operate, including those governing air emissions, water discharge, waste disposal, hazardous materials, and land use.

4.2 Greenhouse Gas Emissions Disclosure

Teradata is required to report on third party greenhouse gas (GHG) emissions as part of its CSRD and CDP obligations. To support this:

- All Third Parties are expected to disclose their Scope 1 and Scope 2 GHG emissions annually upon request by Teradata
- Large or high-spend Third Parties are expected to provide an emissions reduction roadmap within 18 months of this Code taking effect

Teradata will work with Third Parties to identify appropriate disclosure frameworks and tools. Where a Third Party uses a recognized platform (e.g. CDP supply chain, EcoVadis) to disclose emissions data, this may satisfy Teradata's reporting requirements.

4.3 Climate Targets and Reduction

Third Parties are encouraged to set and publicly disclose emissions reduction targets consistent with limiting global warming. Over time, Teradata will favor Third Parties that show clear climate commitments and measurable emissions reductions.

4.4 Waste and Resource Management

Third Parties must manage waste responsibly, implementing recycling and resource efficiency programs where feasible. Third Parties involved in the manufacture, distribution, or disposal of hardware or electronic equipment must comply with all applicable e-waste regulations and handle electronic waste through certified and responsible recycling channels.

4.5 Responsible Mineral Sourcing

Third Parties that supply hardware or physical components to Teradata must support responsible mineral sourcing and exercise due diligence to ensure that materials supplied do not directly or indirectly finance armed groups or contribute to human rights abuses, in accordance with Teradata's Conflict Minerals Policy. This provision applies to Third Parties supplying hardware or physical components; it does not apply to software, services, or professional services Third Parties.

5. Responsible Business Practices

5.1 Third Party Transparency and Cascade

Third Parties must disclose to Teradata, upon request, the identity of their own critical sub-suppliers involved in delivering goods or services to Teradata. Third Parties are expected to use commercially reasonable efforts to communicate the standards of this Code to their own critical suppliers and to encourage equivalent conduct throughout their supply chains.

Teradata recognizes that supply chain due diligence varies in depth and maturity. Expectations will be applied proportionately based on a Third Party's size, risk profile, and supply chain complexity.

5.2 Responsible Sourcing

Third Parties must source materials and services responsibly, avoiding suppliers with known and unaddressed human rights or significant environmental violations. Third Parties should conduct proportionate due diligence on their own third parties and partners, commensurate with the risk profile of the materials and regions involved.

5.3 Political Activities

Third Parties must not make political contributions or engage in political activities on behalf of or in connection with Teradata. Any political activity by a Third Party in its own capacity must be clearly separated from its role as a Teradata third party.

5.4 Business Continuity

Third Parties providing material services to Teradata must maintain appropriate business continuity and disaster recovery plans proportionate to the services they provide. Third Parties should notify Teradata promptly of any material disruption that may affect service delivery.

6. Compliance and Administration

6.1 Equivalent Ethics and Compliance Programs

Teradata recognizes that many Third Parties already have their own ethics and compliance (E&C) programs and may be subject to industry codes or equivalent standards. Teradata's

approach is not to impose duplicative processes on Third Parties whose own programs effectively meet or exceed the standards in this Code.

A Third Party may demonstrate compliance with this Code through its own E&C Program if the program is no less stringent than this Code and covers the same substantive topic areas. To qualify, a Third Party's own program must:

- Cover all the material topic areas addressed in this Code
- Be subject to internal or external review at least annually
- Be supported by documented policies, training records, or equivalent evidence

6.2 Self-Assessment and Monitoring

All Third Parties may be required to confirm awareness of this Code as a condition of onboarding and contract renewal. Third Parties may be required to complete a periodic self-assessment questionnaire (SAQ).

Third Parties are expected to self-monitor their adherence to this Code and to notify Teradata promptly of any identified non-compliance or material change in circumstances that may affect their ability to comply.

6.3 Right to Audit

Teradata reserves the right to review, assess, or audit a Third Party's compliance with this Code, applicable Teradata policies, contractual obligations, and applicable laws.

Third Parties must cooperate fully with such audits, providing complete and accurate information, certifications, documentation and access to relevant records, systems, facilities, and personnel.

Falsification, concealment, or destruction of records, refusal to cooperate, or failure to address material compliance concerns may result in corrective action, suspension, or termination of the business relationship.

6.4 Breach and Remediation

Where Teradata identifies a breach of this Code, or where a Third Party self-reports a breach, the following response will apply:

- Step 1 — Written notice: Teradata will notify the Third Party in writing of the identified breach and the required corrective action where corrective action is feasible
- Step 2 — Corrective action plan (CAP): The Third Party must submit a CAP within 30 days (or such other period as Teradata reasonably agrees), with agreed milestones for remediation
- Step 3 — Enhanced monitoring: Teradata may impose enhanced monitoring or reporting obligations during the remediation period
- Step 4 — Suspension or termination: Where a Third Party fails to remediate within the agreed timeframe, or where the breach is sufficiently serious or repeated, Teradata reserves the right to suspend or terminate the business relationship

Teradata will apply this process proportionately, considering the severity of the breach, the Third Party's cooperation, and the risk to Teradata and its stakeholders.

In the event of an actual or suspected security incident involving Teradata data or systems, Third Parties must notify Teradata without undue delay, and in any case no later than 24 hours after becoming aware of the incident, unless otherwise specified in the applicable contract. Notification should be directed to information.security@teradata.com.

6.5 Reporting Concerns

Third Parties, their employees, and others may report suspected violations of this Code, or seek guidance on ethics and compliance matters, by reaching out to Teradata's Ethics and Compliance Office at E&C@teradata.com.

Teradata also maintains an Ethics Helpline that is:

- Accessible 24 hours a day, 7 days a week
- Available in multiple languages
- Administered by an independent third party
- Able to accommodate anonymous and confidential reporting, to the extent permitted by applicable law

The Helpline may be reached by telephone at **+1-866-455-0993** or online.

6.6 Non-Retaliation

Teradata will not retaliate against any Third Party or individual who raises a concern or reports a potential violation in good faith. Third Parties must uphold the same principle for their own workers and must not discipline, dismiss, or otherwise penalize any person who raises concerns in good faith through any lawful channel.

6.7 Document Governance

This Code is reviewed annually by Teradata's Sourcing and Procurement team in coordination with the ESG and Legal functions. Material changes will be communicated to Third Parties with a minimum 90-day transition period before taking effect.

Version	2.0
Effective date	July 2026
Next review	July 2027
Owner	Teradata Sourcing and Procurement / ESG
Contact	supplier.onboarding@teradata.com

Appendix: Definitions and Reference Standards

A. Key Definitions

Third Party — Any entity or individual providing goods, services, or expertise to Teradata, including distributors, resellers, vendors, consultants, contractors, staffing agencies, and marketing representatives.

Worker — Any individual performing work for or on behalf of a Third Party, including permanent employees, temporary staff, agency workers, apprentices, interns, and migrant workers.

Sub-supplier — Any entity engaged by a Third Party to perform work that is material to the delivery of goods or services to Teradata.

Material Third Party — A Third Party that is significant to Teradata's operations by virtue of spend, business criticality, geographic risk, or ESG risk profile, as determined by Teradata's risk tiering process.

Corrective Action Plan (CAP) — A documented plan agreed between Teradata and a Third Party setting out the steps and timelines for addressing an identified compliance breach.

B. Referenced International Standards

This Code draws on the following internationally recognized frameworks, all of which are freely referenceable and require no Teradata membership:

- ILO Core Conventions — Conventions 29, 87, 98, 100, 105, 111, 138, 182 (forced labor, freedom of association, equal remuneration, discrimination, child labor)
- UN Guiding Principles on Business and Human Rights (UNGPs) — the foundational framework for business human rights due diligence, endorsed by the UN Human Rights Council
- OECD Guidelines for Multinational Enterprises — government-backed responsible business conduct standards covering human rights, labor, environment, and anti-corruption
- ISO 14001 — international standard for environmental management systems
- ISO 45001 — international standard for occupational health and safety management systems
- ISO 27001 / SOC 2 — international standards for information security management
- GRI Standards — Global Reporting Initiative standards used by Teradata for sustainability reporting (GRI 205, 305, 306, 408, 409)

C. Teradata Policies Referenced in This Code

- Teradata Code of Conduct
- Teradata Global Anti-Corruption Policy
- Teradata Global Privacy Statement

- Teradata Conflict Minerals Policy
- Teradata Human Rights Statements
- Teradata Modern Slavery and Human Trafficking Statement
- Teradata Ethics Helpline

17095 Via Del Campo, San Diego, CA 92127 | Teradata.com

Teradata and the Teradata logo are registered trademarks of Teradata Corporation and/or its affiliates in the U.S. and worldwide.

Copyright © 2026 by Teradata Corporation. All Rights Reserved.