

Rising above

Teradata Corporation Code of Conduct

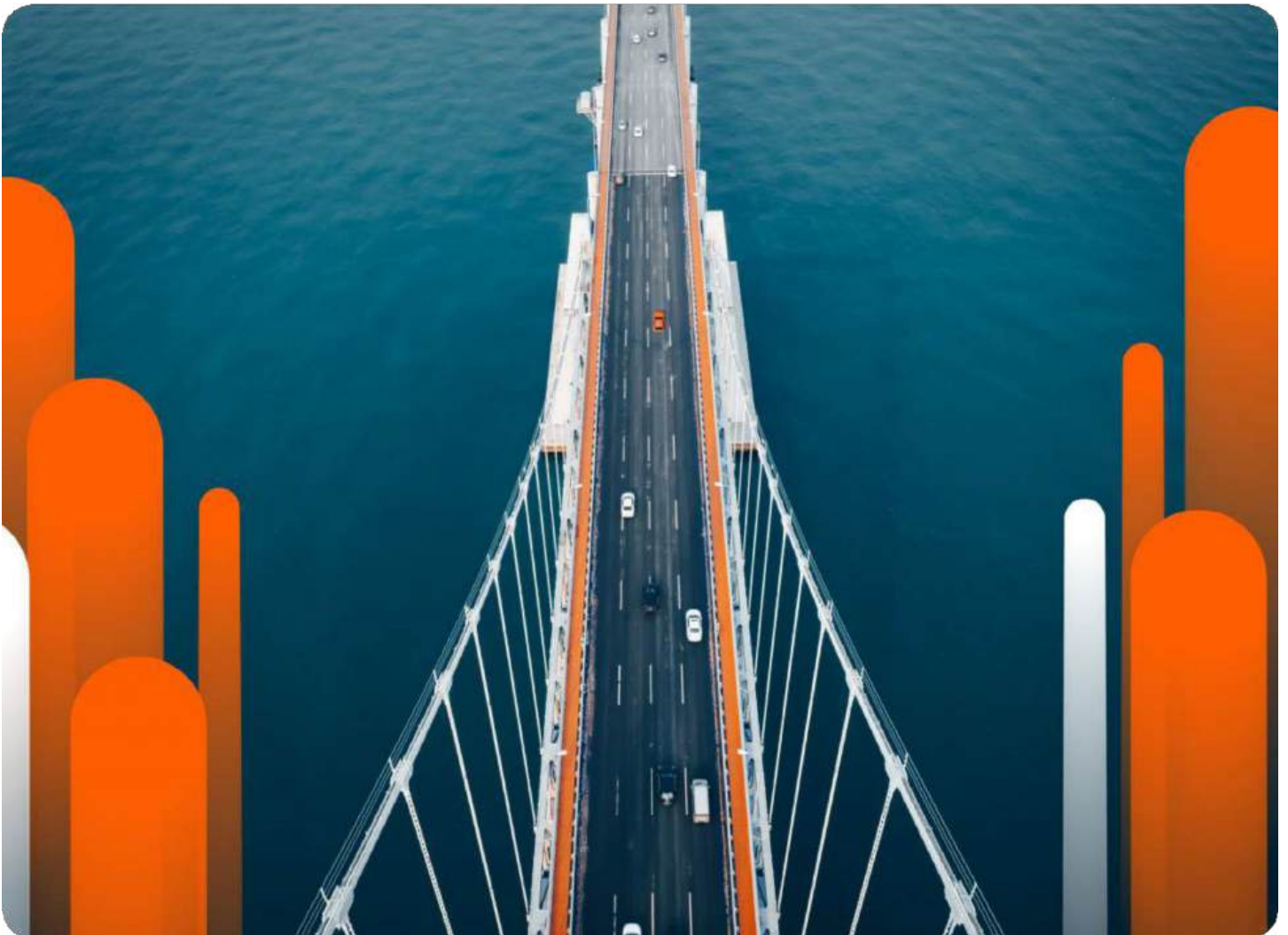


Table of contents

- 4 Integrity matters**
 - Letter from leadership
- 5 Upholding the Code**
 - Who must follow the code?
 - Our Code of Conduct commitments
 - Using the Code to make ethical decisions
 - Seeking guidance and reporting violations
 - Investigating reports of suspected violations
 - Non-retaliation
 - Special responsibilities of managers
- 8 Accountability to each other**
 - Diversity, equity, and inclusion (DEI)
 - Non-discrimination, non-harassment, and anti-bullying
 - Avoiding conflicts of interest
 - Workplace safety and health
 - Use of company assets
- 13 Reaching out to the public**
 - Keeping accurate records
 - Social messaging, IT, and network systems
 - Insider trading
 - External company communications
 - Political and charitable activities
- 17 Honoring our commitments**
 - Zero tolerance for bribery and corruption
 - Export and import compliance
 - Gifts and entertainment
 - Environmental, health, and safety (EH&S)
 - Social responsibility and human rights
- 22 Pursuing innovation**
 - Proprietary and confidential information
 - Third-party intellectual property
 - Teradata Certification Program
 - Privacy and data protection
 - Artificial intelligence (AI)
- 25 Rising to the top of our industry**
 - Competing fairly
 - Participating in industry associations and trade shows
 - Dealing fairly with customers
 - Not abusing market power
 - Business intelligence
- 28 Ethics and compliance contacts and resources**

At Teradata, we know that people thrive when empowered with trusted information. Trust accelerates opportunity, paving the way for innovation and partnerships. Together, we enable our customers and our world to rise above. The Teradata Code of Conduct (also referred to as “Code”) is a summary of the standards of conduct that all Teradata people and teams must follow to help us rise even higher. The Code helps us understand how to comply with the legal and ethical responsibilities that come with our jobs. It also helps Teradata establish clear and consistent rules for everyone to follow.

The Code is only a general overview. You will find several policies referenced in the Code and elsewhere in Teradata communications. These policies establish, in more detail, our requirements. We also outline the reporting of suspected violations. You should feel comfortable asking questions before you act so you can get clear answers in advance about complying with our Code, our policies, or legal requirements. The Code should be applied consistently with our Core Principles of being customer and market driven, agility in execution, and accountability to each other.

Our Code of Conduct applies to all Teradata people and organizations globally. In this document, “Teradata” refers to Teradata Corporation and all its subsidiaries, affiliates, business organizations, teams, and operations throughout the world. Teradata “associates” include every Teradata employee, independent contractor, subcontractor, temporary employee, agent, representative, officer, and board member.

Teradata “business partners” include every Teradata supplier, vendor, reseller, distributor, alliance partner, service provider, and other third party with whom Teradata conducts, or proposes to conduct, business. Teradata “people” are all Teradata “associates” and all Teradata “business partners” throughout the world.

Teradata Global Policies

Employees of Teradata have access to our Global Policies website at <https://teradata.sharepoint.com/teams/policy>, where each of the policies referenced in the Code can be found.

Integrity matters

Our commitment to ethical excellence at Teradata

We are in an era of incredible technological transformation driven by AI. As the most open and connected platform for data analytics and Trusted AI, Teradata plays a vital role in enabling enterprises to navigate the AI revolution, delivering harmonized data and faster innovation. And as a company, we remain focused on growth and innovation while upholding our unwavering commitment to doing business ethically.

Our strong ethical culture is the outcome of good business practices demonstrated across the organization through choices we make daily. As we continue to execute on our strategy, our Code of Conduct steers our planning, processes, and decision-making, and is an extension of our Core Principles of accountability to each other, agility in execution, and being customer and market driven.

At Teradata, integrity is everyone's job. Our Board of Directors and senior leadership continuously prioritize ethics and integrity, and employees are held accountable to our high standards. We act promptly and decisively in response to any compliance infringements.

With the collective commitment of our employees, we have earned our reputation for integrity, allowing Teradata to be recognized as "One of the World's Most Ethical Companies" for many consecutive years. As we continue on our journey of success, we invite each of you and our community of partners and suppliers to commit personally to upholding the Code of Conduct and our Core Principles in all Teradata-related business.

Thank you for ensuring that ethics, compliance, and integrity remain at the center of everything we do at Teradata, as we continue to thrive as an organization that values trust, respect, and shared purpose.

Steve McMillan

President and Chief Executive Officer
Teradata Corporation

Angie Snavelly

Senior Vice President, Corporate, Ethics &
Compliance Officer, & Assistant Secretary
Teradata Corporation

Upholding the Code

Our Code expresses what Teradata expects from our associates, business partners, and broader team. Trust has been placed in us to do the right thing. We earn that trust by asking questions and getting answers before we act, and by rising against wrongdoing. We earn it by upholding Teradata's reputation as a customer-dedicated, passionate company that does business the smart way and the right way. And, as we earn trust, we continue to build a bright future for our company, our shareholders, our business partners, our communities, and our customers.

If something doesn't feel right, doesn't seem right, doesn't look right, or doesn't sound right, we must question it. If our Code and policies don't clearly address a concern, we must seek guidance from other sources. We must continuously earn and confirm trust by doing the right thing.

Who must follow the code?

The Teradata Code applies to all Teradata teams throughout the world. We also expect our business partners to comply with our standards of conduct with respect to all their Teradata-related activities.

Teradata subsidiaries, affiliates, business organizations, operations, and teams may decide to implement additional standards to supplement our Code. If supplemental standards apply to you, you must always follow the stricter standard so that you comply with both our Code and team- or role-specific standards.

By incorporating our Code into our daily activities, we will help ensure we do business the right way. Anyone who acts contrary to the principles and standards established by our Code will be subject to discipline, up to and including termination, consistent with local law.

Our Code of Conduct commitments

We conduct business ethically and in compliance with our Code and policies.

We use our Code as a guide to upholding our Core Principles.

We seek guidance and report concerns and violations.

We treat all people with respect.

We comply with laws.

We compete fairly.

We avoid conflicts of interest.

We protect assets.

We protect data and personal information.

We keep accurate records.

We apply our Code and policies consistently.

We prohibit retaliation against those raising concerns in good faith.

We do the right thing—always.

Using the Code to make ethical decisions

Our Code sets the standards for how we conduct Teradata business. However, our Code and policies are only guides to ethical conduct. They cannot cover every possible situation or every question a Teradata person might face. If you are unsure about what is the right thing to do, you should ask. Ethics compel us to get an answer before we act if we are uncertain if something is right.

On unique occasions, it may be appropriate to waive or alter a provision of our Code or a policy for a unique situation. This might be the case if doing one thing would be a violation but doing another thing—or nothing at all—would also be a violation, or where legal requirements changed after the provision was written. If you encounter circumstances where you think such an ethical dilemma or contradiction has arisen, you should raise the issue immediately. See “Seeking Guidance and Reporting Violations” below. The important thing is to obtain direction before you act if you face such a dilemma or uncertainty.

Except for permitted deviations expressly provided for in our policies, all Code and policy waivers require the advance written approval of the Teradata Law Organization. Only the Audit Committee of the Teradata Board of Directors may waive compliance with our Code by Teradata executive officers or board members, only in the most unique situations, and only in compliance with proper disclosure and transparency requirements. We hold everyone from the top down to the same standards of conduct.

And we hold company executives and board members to even higher standards and expectations.



Seeking guidance and reporting violations

Violations of our Code are serious and can cause great harm to our business relationships and reputation. If you have a question or concern, or you become aware of conduct you think may be a violation of our Code, our policies, or the law, then you have a duty to speak up. Reporting your concerns in good faith—meaning you are giving a sincere and complete account of a possible issue—helps Teradata avoid or solve problems in the workplace before they escalate.

If you suspect a legal or ethical violation, bring it to the attention of one of the following:

- Your manager (if you are comfortable raising your concern with your manager)
- A higher-level manager
- Your Teradata People Organization representative
- The Teradata Ethics & Compliance Office by email at E&C@Teradata.com
- The Teradata Ethics Helpline, which can be reached online at www.integrity-helpline.com/tdhelp.jsp or by telephone at **1-866-455-0993**. The helpline telephone number is printed on most Teradata associate identification badges, so it is available to you at all times. The helpline allows for anonymous reporting, where permitted by law.
- Any member of the Teradata Law Organization
- A member of the Teradata subject matter expert team for the area at issue (for example, Corporate Security for suspected theft issues, or Internal Audit for suspected financial irregularities)

While you may choose to report anonymously, it may be difficult to follow up with specific details of your concern. In some countries, local laws may require you to identify yourself. The Ethics & Compliance Office or the Ethics Helpline will let you know if either of these applies to your report. We encourage you to identify yourself when contacting these resources so Teradata can thoroughly investigate the issue. If you do give your name or come forward in person, Teradata will take steps to the fullest extent permitted by applicable laws to protect your identity, sharing your name only on a need-to-know basis.

Investigating reports of suspected violations

When you raise a business conduct concern, Teradata takes it seriously. We thoroughly analyze and investigate all reports of suspected misconduct while handling your personal information discreetly. No matter their level of seniority or role at Teradata, anyone who violates the Code, our policies, or laws will be subject to appropriate disciplinary action, up to and including termination of employment, unless prohibited by local law. You can read about how we handle [investigations here](#).

If asked to aid in an investigation, you must answer all questions truthfully and cooperate completely. Lying, concealing, or covering up an ethical or legal violation is a serious violation of our Code and may result in termination of employment.

If you do not feel comfortable reporting your concerns

to any of the resources listed here, you may report them directly to the Audit Committee of the Teradata Board of Directors by written communication to the Corporate Secretary at the Teradata world headquarters: Audit Committee of the Board of Directors, Teradata Corporation, Attention: Corporate Secretary, 17095 Via Del Campo, San Diego, California (USA) 92127.

Non-retaliation

All Teradata people must feel empowered to report any suspected violation of the law, our Code, or Teradata policies without fear that their employment or other business relationship with Teradata will be negatively impacted. Teradata fosters an environment of “see something, say something.” To reinforce this, Teradata strictly prohibits any form of retaliation against those who ask questions, voice concerns, or submit reports in good faith, as well as those who participate in ethics and compliance investigations and audits.

Retaliation is any negative consequence that you might experience as a result of making a report, participating in an investigation, or asking a question. This might include being inappropriately demoted, getting an unfairly negative performance evaluation, or receiving an unjustified reduction in your bonus or pay. It can also include more subtle actions, like being intentionally left out of important

projects or meetings. If you think you have experienced or witnessed retaliation, contact one of the resources listed above. By reporting retaliation, you are taking a stand for ethics and integrity in our workplace and making Teradata a better place to work.

Good faith does not mean you have to be right, but it does mean you are providing all the information you have, and you believe it to be truthful. Bad faith is when someone provides information they know is false, often with the intent to target or retaliate against someone else. Just as we do not tolerate retaliation, we will not tolerate knowingly false information submitted in bad faith.

Special responsibilities of managers

Teradata associates who supervise others have additional duties and responsibilities. Managers must show, through their words, decisions, and actions, a personal commitment to the highest standards of integrity. As a Teradata manager, you are expected to:

- Set an example by always following the Code and Teradata’s policies yourself
- Ensure, through discussion, communication, and training, that associates on your team and your business partners understand our Code and relevant policies
- Consider whether associates on your team demonstrate adherence to our Code and exemplify Teradata’s Core Principles before promoting them to positions of greater responsibility
- Recognize and reward associates who set positive examples through their actions and behaviors
- Be alert to, and, as necessary, report any potential misconduct that occurs within your team or workplace to the Teradata Ethics & Compliance Office
- Create an environment that encourages Teradata people to raise ethics, compliance, and policy questions and concerns
- Never take or allow retribution against those who raise concerns in good faith

Managers who know or should have known about violations and do not address and/or report them may be subject to discipline. Remember: as a Teradata manager, it is your duty to set the tone that integrity is a top priority at Teradata.

Accountability to each other

We seek to provide a work environment at Teradata that fosters respect for all associates, customers, and business partners and that includes and reflects the diversity of the communities in which we operate. We back up this promise with our policies against discrimination, harassment, bullying, and retaliation. We have also declared our position as an anti-racist company, which includes our support for extinguishing any system, value, behavior, or process that inadvertently perpetuates racism or other inequalities within our organization.

Diversity, equity, and inclusion (DEI)

As a global company, Teradata understands that its diversity of people—and the culture, ideas, training, and background they provide—enable us to drive innovation and enhance the products and services we deliver to our customers. When we cultivate a safe, collaborative and inclusive environment, that enables everyone at Teradata to achieve their full potential.

Teradata complies with the laws and regulations of the countries in which we operate. However, our commitment to DEI extends far beyond legal compliance. Teradata strives to create a workplace where different cultures and ideas are valued, supported, and encouraged. Teradata regularly examines its policies, systems, and working conditions to ensure there is equal opportunity and that we are inclusive in our actions. We also provide learning opportunities to all employees covering topics relating to culture, inclusive leadership, managing bias, and fair treatment for all. Teradata's Inclusion Communities offer networking and mentoring support for employees of various backgrounds. Additionally, Teradata seeks to integrate supplier diversity into its procurement process by identifying and purchasing from businesses that embrace diversity. However, our work is not finished, and Teradata is committed to continuous growth and achievement in this area.

Non-discrimination, non-harassment, and anti-bullying

At Teradata, we are deeply and genuinely committed to a workplace with no discrimination, harassment, or bullying. We are committed to combatting and eliminating all forms of discrimination including racism, which may be defined as actions, behaviors, or words, direct or indirect, which marginalize, exclude, and discriminate against individuals on the basis of their membership in a particular racial or ethnic group.

Teradata prohibits unlawful discrimination in any decision-making, including in employment-related decisions or business partner selection decisions. We hire, select, give performance appraisals, and promote based on merit—never discriminating against anyone on the basis of protected characteristics such as race, color, religion, national origin, gender, age, disability, sexual orientation, pregnancy, gender identity, gender expression, marital status, military or veteran status, or any other legally protected characteristic. We do not tolerate behavior that results in discrimination based on these or other protected characteristics. We are also committed to eliminating practices and procedures that may result in unintended or inadvertent discrimination.

Respect for one another also demands a work environment free from all forms of unlawful harassment and bullying. Harassment is unwanted or offensive conduct towards another person based on protected characteristics when: (1) submission to such conduct is either made an explicit or implicit condition of employment or is used as the basis for an employment decision; or (2) the conduct is so severe or pervasive that it creates an intimidating, hostile, or offensive work environment. Harassment can be sexual or nonsexual in nature. Sexual harassment involves unwelcome sexual advances, requests for sexual favors, or other physical or verbal conduct or workplace behaviors of a sexual nature.

Although there is no legal definition of bullying, it can be described as unwanted behavior from a person or group that is either offensive, intimidating, malicious, or insulting; or an abuse or misuse of power that undermines, humiliates, or causes physical or emotional harm to someone. Bullying might be a regular pattern of behavior or a one-off incident; it might happen face to face, on social media, in emails or

Our pledge to diversity, equity, and inclusion

We will encourage all to speak up when they experience or witness intolerance, mistreatment, incivility, or conscious/unconscious bias action.

We will ask ourselves, “Do our actions and words reflect the value of inclusion?”

We will initiate meaningful, complex, and sometimes difficult conversations with colleagues.

We commit to ensuring an inclusive environment for all. We will see different perspectives and respect points of view and communications styles that are different from our own.

We will ensure our actions and words reflect the value of and our commitment to inclusion.

We will encourage all to move outside our comfort zones to learn about the experiences and perspectives of others.

Teradata is an anti-racist company. In addition, we are committed to be an anti-racist company in which we identify and extinguish any system, value, behavior, or organizational process that perpetuates systemic racism. To do this, we commit to:

Actively contribute to a culture in which racism is not accepted.

Acknowledge and confront incidents of racial discrimination and provide support for the employees who were negatively affected.

Engage in ongoing opportunities to learn about the importance of diversity, equity, and inclusion, including our collective responsibility with respect to anti-racist behaviors and processes.

By committing to these behaviors and actions, together we will create an environment where employees feel safe and free from discrimination and racism.

calls, at work, or in other work-related situations; and it may not always be obvious or noticed by others. No matter the form they take, harassment and bullying can interfere with a person’s work performance or adversely affect a person’s employment opportunities. Teradata does not tolerate harassment or bullying regardless of whether they occur on company premises; during off-site or after-hours events such as holiday parties, team-building events, celebrations, business conferences, or business travel; or whether they occur online over internal communication tools or internal or external social media platforms.

At Teradata, we take very seriously all reports and concerns regarding possible workplace discrimination, harassment, and bullying, including incidents of racism or sexual harassment. If you believe you are experiencing discrimination, harassment, or bullying, or if you become

aware of a situation that violates our policies against discrimination, harassment, or bullying, you should report it immediately using the reporting methods outlined in our Code. Managers who receive complaints of potential misconduct, or who observe possible discrimination, harassment, or bullying, must escalate the complaint or misconduct immediately to a member of Teradata’s People Organization or the Teradata Ethics & Compliance Office so that an investigation can be conducted and appropriate corrective action taken.

Teradata welcomes the opportunity to identify, investigate, and resolve concerns early before they become more serious issues. Teradata strictly prohibits retaliation against anyone who makes a good-faith report based on a reasonable belief of discrimination, harassment, or bullying.



Red flags of sexual or other harassment

Offensive, inappropriate, demeaning, or unwelcome comments, jokes, or images connected with the workplace (including in emails and other electronic communications using company resources) regarding sexual conduct, sexual attractiveness, sexuality, sexual orientation, gender identity, age, race, national origin, religion, disability, pregnancy, or other legally protected characteristic are prohibited.

Zero tolerance for racism

Telling a racist joke; using a racial epithet or symbol; demonstrating behavior that reflects the idea of inherent superiority of one ethnic group over another group; or racial profiling are examples of behavior that is prohibited by Teradata.

Avoiding conflicts of interest

We are all dedicated to making Teradata successful. Conflicts of interest can interfere with our success. Conflicts can develop when our personal, family, or financial interests interfere (or even appear to interfere) with our ability to make objective business decisions in the best interests of Teradata. We all must avoid any situation where we feel torn between our loyalty to Teradata and outside interests.

Here are some examples of common conflict situations. If you have a real or potential conflict of interest, disclose it to your manager right away. While a particular potential conflict situation may not rise to the level of a Code violation, failure to report a conflict may.

Doing business with family and friends

A conflict of interest may arise if you (or your spouse, relative, or close friend) have a personal stake in a company that supplies or seeks to supply goods or services to Teradata; is a Teradata customer or prospect; or competes with Teradata. If you find yourself in that situation, you must not use your position to influence the selection or bidding process or negotiations involving that party. If you are directly involved in vendor selection, and the potential conflict involves a vendor or potential vendor, you must notify your manager immediately and remove yourself from the decision-making process. You should also not be involved in assessing the quality of the goods or services provided if the vendor with whom you have a relationship is selected.

If you have a relative or close friend who works for a competitor, notify your manager; take extra precautions

to avoid giving the relative or friend access to Teradata confidential information and information systems; and avoid communicating with them about things covered by our competition/antitrust law compliance and insider-trading Code provisions and policies.

A romantic relationship between a representative of a seller and a representative of a buyer also raises conflict of interest issues that must be disclosed and addressed before any transaction including their employers is completed.

Teradata's policy on employment of family members (**Corporate Management Policy (CMP) 201**) generally prohibits us from hiring, supervising, or otherwise overseeing a family member or a person with whom we have a romantic relationship. If you have or are aware of any such conflict, then you must report it immediately to your manager and the Teradata People Organization representatives so that the hiring, supervisory, and/or overseeing relationship between the two involved people can be changed or otherwise addressed.

Outside employment and investments

Taking employment outside of Teradata or holding a major stake in a Teradata competitor also may create a conflict of interest for a Teradata associate. If you are a full-time Teradata employee, you may not conduct any non-Teradata business that interferes with the proper performance of your employment with Teradata. This includes conducting outside business during your Teradata working hours or using Teradata property, equipment, networks, information, or other resources for non-Teradata business uses. Also, serving on the board of another for-profit or publicly traded company can present conflicts of interest. Teradata associates should raise all new offers of such roles and questions regarding holding major shares in our competitors to their manager and the Teradata Law Organization. We can typically address these situations by communicating about the boundaries, expectations, and requirements of the position and the intended extent of the shareholding.

Corporate opportunities

In some cases, through your position at Teradata, you may become aware of an opportunity to make a purchase or investment in which Teradata might be interested. You must promptly notify your manager of the opportunity to allow Teradata to evaluate it. If Teradata opts not to pursue that opportunity, you must also seek and obtain written approval from your manager and the Teradata Ethics & Compliance Office before you act on it for yourself or refer it to another party.

Handling conflicts of interest

Teradata recognizes a conflict of interest may develop without any bad intentions, and changes in circumstances may arise that create a conflict or the appearance of a conflict of interest where none previously existed.

The important thing to remember regarding this subject is that as soon as you become aware of a possible conflict of interest situation, you must disclose it to your manager. Your manager, working with the Teradata People Organization, the Law Organization, and/or the Teradata Ethics & Compliance Office, will determine what must be done to resolve it, or will give you approval to proceed with assurances you will implement proper precautionary actions so a potential conflict of interest will not become an actual one.



Conflict of interest guidance

Question: Your uncle owns and runs a business that supplies a certain type of service, and you become aware that Teradata is in the market for that type of service. Can you refer the Teradata people involved in procuring that type of service to your uncle's business?

Answer: Yes, but, under our Conflict of Interest Policy, you must disclose your relationship when you make the referral. Also, you must not be involved in the decision-making process to select providers for that service; negotiate, implement, or manage that service if it is procured from your uncle's company; evaluate the quality of the service; or approve payments to your uncle's company. Disclosure, transparency, and removing yourself from the related decision-making, management, and payment channels are keys to being compliant under these circumstances.



Workplace safety and health

Teradata strives to provide each associate and business partner with a safe and healthy work environment. We conduct no activity without taking all proper health, safety, and environmental protection precautions. This applies to office and virtual work locations.

Teradata is also committed to a drug-free workplace. That means all of us must be free from the influence of drugs and alcohol while conducting business. The use, possession, distribution, or sale of illegal drugs, or the improper use or abuse of prescription or other lawful drugs, on company premises or while on company business is strictly prohibited. Alcohol may be consumed in moderation at certain management-approved, company-sponsored events, but only consistent with the guidelines of the event, and only if the associate consuming the alcohol accepts full responsibility and accountability for their consumption and conduct and does not operate a motor vehicle while legally impaired.

Violations of our drug and alcohol abuse policy in the workplace will not be tolerated. Teradata has associate support programs in place to assist associates who are dealing with drug or alcohol abuse or addictions. Affected associates are encouraged to use these programs. Information about these services is available through the Teradata Employee Assistance Program.

Teradata associates are expected to treat each other with respect and courtesy. Teradata will not tolerate acts or threats of violence. If you witness actual or threatened violence in the workplace, you should report it immediately to your manager, facilities manager, or People Organization representative.

Use of company assets

Teradata assets—its information, facilities, equipment, networks, materials, property, technology, and reputation—have been acquired through the hard work, achievement, and dedication of our entire team. We all have an interest in the continued success of Teradata, and we all are accountable for that success. We must protect our assets and associated data and personal information from theft, damage, loss, and misuse, and ensure they are used only for Teradata and Teradata-approved purposes.

Teradata recognizes our associates may occasionally make limited personal use of certain Teradata assets. However, the routine or extensive use of Teradata time, assets, or resources for personal purposes is not permitted. Anything more than minimal use of Teradata resources for personal or non-Teradata-approved community or charitable purposes must receive prior approval from your manager.

If you are in doubt about whether the amount, type, or content of personal use of Teradata assets is proper, please discuss it with your manager, obtain approval in advance, and refrain from using Teradata assets for such purposes until after you have received permission to do so.

The Teradata Code applies to both business use and permitted personal use of Teradata assets. This means you should not use Teradata assets at any time for anything that violates the Code or our policies, such as for accessing, viewing, storing, or sending pornography; engaging in acts of discrimination, harassment, bullying, retaliation, or threats of violence; or illegal gambling, prostitution, or any illegal activities. Violations will lead to discipline, up to and including termination of employment.

Reaching out to the public

Teradata operates in a highly competitive marketplace.

We must constantly innovate and improve our products and solutions to meet our customers' needs and keep pace with our competition. Equally important, we must make sure we are holding ourselves to high standards of behavior and remaining authentic and true in our dealings with the public to show the consistency of our brand and our principles.

Keeping accurate records

All of us are responsible for ensuring Teradata books and records are complete and accurate. All our financial entries and records, including travel, entertainment, and gift expense reimbursement requests and payments; procurement, contractor, and subcontractor purchase orders; contracts, statements of work, entries, and payments; and project finances and reporting must fairly and accurately reflect the true nature, amounts, relevant actual dates, involved parties, and purpose of the spending/transaction or project, as the case may be.

This means we may not establish or use any slush funds, unrecorded pools of money, or unauthorized assets/accounts for bribes, kickbacks, travel, entertainment, gifts, favors, personal items, invoice payments, discounts, rebates, procurement, contractors, subcontractors, contracts, work orders or any other improper purpose. You must never make false or artificial entries on expense reports, purchase orders, invoices or project reporting methods/tools or any other Teradata books and records.

We need accurate information to make the best and most effective decisions for our business. To fulfill our obligations and to be accountable to customers, associates, business partners, shareholders, and government authorities, we must keep full, fair, accurate, and timely books and records of all business transactions. Accurate records are critical to Teradata fulfilling its financial, legal, and reporting obligations.

All Teradata associates are required to make certain that Teradata's books and records are accurate. We need to ensure all the reports we make—including the recording of time worked, business expenses incurred, and all other business-related activities—and all receipts and other supporting documentation, dates and information are not falsified, misleading, or forged in any way. You must record and file reports on time and accurately. If, after checking relevant Teradata policies, you are unsure whether a certain expense is a legitimate reimbursable/payable business expense or is permitted by our policies, you should ask your manager or other subject matter experts in the company before you act and before you submit a reimbursement/payment claim for it. Associates are accountable and will be



subject to discipline for submitting false reports or claims for reimbursement/payment.

We must never book or process a transaction or payment, including recognizing orders and recognizing revenue, without the full and appropriate underlying documentation. Falsifying, forging, or back-dating books, records, orders, contracts, approvals, invoices, acceptances, or any documents that may be used in connection with revenue recognition or other proper accounting treatment is always wrong and will not be tolerated. Each of us must cooperate fully with financial controls personnel, revenue recognition assurance personnel, and internal and external auditors in their effort to verify the accuracy of the company's books and records and compliance with accounting and legal requirements. Refusing to cooperate, offering misleading information, or affirmatively interfering with a review, audit, or investigation will result in discipline.

Properly maintaining corporate records after they are created also is very important. Teradata has adopted a Record Retention Policy (**Corporate Finance & Accounting Policy (CFAP) 111**) describing how to maintain records for required periods and destroy them when they are no longer needed. If you are unsure about what records you need to maintain and for how long, please review our Record Retention Policy and make certain you follow the record retention schedule for your area or for the types of documents with which you work.

Also keep in mind that in the event of actual or threatened legal proceedings or government investigations, a legal hold might be placed on certain documents and records.



Teradata's status in legal proceedings may be at risk if we do not secure or are unable to produce relevant documents and records. In these cases, you will be contacted by the Teradata Law Organization. If a legal hold applies to you or documents or records held or controlled by you, you must retain all relevant records subject to the legal hold instructions.

Red flags of fraud

- The individual is in the office at odd hours for no apparent legitimate business purpose
- The individual is discreetly accessing/copying company records for no apparent legitimate business purpose or reason related to their job responsibilities
- The individual's lifestyle reflects that they are living beyond their means
- The individual lacks personal stability; is experiencing an emotional trauma in home life or work life; or is facing undue/unreasonable family, company, community, financial, or lifestyle expectations
- The individual consistently tries to beat the system, compromise or manipulate processes, or exceed their authority
- An unnecessary intermediary/contractor is used; an unqualified or not-fully-vetted intermediary/contractor is used; an associate has an undisclosed personal relationship or arrangement with an intermediary or contractor
- Descriptions or dates on invoices, purchase orders, or statements of work do not match the items involved and/or dates delivered; or invoices or purchase orders for one transaction set are split into multiple invoices or purchase orders to avoid obtaining higher-level approvals that would be otherwise required
- Transferring of Teradata information/assets/data to personal email accounts without prior approval; or use of personal email instead of Teradata email accounts



Social messaging, IT, and network systems

Social networking and the Internet are key business tools. The use of the Internet and social networks at work or using company technologies must be consistent with the Code, our Core Principles, and company policies. We may not use Teradata information technologies (equipment, software, or networking resources) or a customer's or business partner's information technologies to gather or distribute offensive, sexually suggestive, discriminatory, harassing, pornographic, unlawful, or other inappropriate data or information, whether during or after work hours.

How you conduct yourself on social media not only reflects on you—it can be a reflection on Teradata. Only a limited number of people are authorized to speak on behalf of the company. Do not overstate your authority to speak for Teradata. Email messages, text messages, instant messages, blog comments, Twitter messages, social networking site communications, and voicemail messages produce easily forwarded, traceable, and recoverable records of communications. All messages that are related to Teradata and/or made on or through Teradata IT systems, devices, or networks should be composed with the same care you would take in composing a letter on the company's letterhead.

You should assume that whatever you say in emails, instant messages, text messages, and other forms of social networking will be seen by others and could be the subject of external and internal investigations or subject to legally required disclosures. A good rule of thumb to keep in mind

is the “newspaper rule”: If your communication appeared on the front page of the newspaper for others to read without any other context, would it be perceived as consistent with Teradata's Core Principles and Code of Conduct? If not, then don't use it, send it, or post it.

To maintain the security, integrity, and business purposes of our information technologies and comply with laws, regulations, privacy obligations, and contractual duties, we all need to take necessary actions to safeguard passwords and identification codes to prevent unauthorized access to Teradata, customer, and business partner information systems.

Teradata reserves the right to monitor your use of Teradata systems and resources as well as the content of any messages or documents transmitted or stored through or in its systems. This includes information that has been deleted by users or sent over Teradata networks. You should not expect privacy (beyond that required by applicable laws) when using email, the Internet, or other forms of electronic storage or communications on Teradata, customer, or business partner computers or networks. Teradata expects and requires each of us to be respectful of the conditions and limitations that apply to the use of Teradata resources and the resources of its customers and business partners.

None of the restrictions relating to social media or confidentiality of employee information are intended or should be interpreted as limiting an employee's right to engage in legally protected concerted activity.

Insider trading

We regularly have access to information that others may not have about Teradata and the companies with which we conduct or may propose to conduct business. This knowledge may include non-public information that might influence an investor to buy, sell, or otherwise trade in a company's securities (including stocks and options of Teradata or other companies involved), such as non-public information about acquisitions, divestitures, management changes, or financial results or projections.

Insider trading is the illegal act of buying, selling, or otherwise trading in securities while in the possession of material non-public information about Teradata, its customers, its business partners, or others with which Teradata has or is considering a business relationship. Insider trading is a serious violation of our Code, the Teradata Insider Trading Policy (see Corporate Management Policies **CMP 922** and **CMP 922Q**), as well as state and federal securities laws, and could subject the individuals involved to immediate termination and potential criminal prosecution.

"Tipping" is also a violation of our policies, Code, and securities laws, with the same consequences. Tipping occurs when you provide material non-public information to someone else, even inadvertently, and that person acts on the information or tips others to act on the information to buy, sell, or otherwise trade in securities. Each of us must be careful not to disclose any non-public information about Teradata, its customers, its business partners, or others with which Teradata has or is considering a business relationship to family members, friends, or other third parties.

Under the Teradata Insider Trading Policy, certain associates will be treated as restricted insiders and automatically "blackout" from trading during certain periods. If you have questions or concerns about trading in securities while in possession of inside information or while serving in a restricted insider role, consult the Teradata Insider Trading Policy, and, if still in doubt, contact the Law Organization for more guidance before you trade.

External company communications

To help ensure our reputation is effectively managed and protected, all communications with media outlets involving or concerning Teradata must be handled through the Teradata Public Relations/Communications organization. Similarly, all responses to subpoenas and governmental inquiries and inspection requests must be handled through the Teradata Law Organization. All business and financial results disclosures must be made only when and as authorized under Teradata policies (see **CMP 110**) and by the Teradata Disclosures Committee. This helps us ensure the information we communicate or produce is consistent, accurate, and in line with Teradata policies and disclosure laws, regulations, and legal requirements.

Political and charitable activities

Teradata associates are encouraged to participate in community and political activities of their own choosing. However, any political involvement must be done on your own time, using your own resources, and not represented as being associated with the company or on the company's behalf unless expressly authorized—in advance—by the Teradata Law Organization.

The laws and regulations governing political contributions and political activities by corporations in many of the places where Teradata does business vary and can be complex. As a general rule, we may not do anything that would make it appear that Teradata is supporting a candidate for election, political party, or political initiative without the advance written approval of the Teradata Law Organization. Even then, the permissible level of political activities will be determined by Teradata's Corporate Political Activity Policy (see **CMP 926**) and external-facing Political Activity Policy Statement located at <https://www.teradata.com/About-Us/Corporate-Governance/Political-Activity-Policy-Statement>.

As a company, we have adopted initiatives and policies in which we support charities and the communities in which we operate. Our company also has a program, Teradata Cares, that, among other things, offers and encourages each of us to use company paid time off to perform charitable/community volunteer service. The amount of Teradata resources used for such purposes must be managed, implemented, and prioritized. This helps us stay on track and avoid conflicts. If you are in doubt about whether your use of company resources or company work time for a charitable or community purpose is permissible or appropriate, please discuss it with your manager and/or the People Organization representative in advance and follow their guidance.

Honoring our commitments

Teradata is a global team of dedicated individuals.

We earn our customers' business and partnership through our dedication to being the best in our field.

To safeguard our reputation, we must obey the laws of the communities in which we operate and respect the customs and traditions of those communities. At the same time, we must not engage in any conduct that violates our Code or policies—even if that conduct would be allowed by local laws.

Zero tolerance for bribery and corruption

We do business free of corruption and other impropriety. Teradata and all its people and teams everywhere in the world are subject to anti-corruption, anti-bribery, and anti-money-laundering laws, including the United States Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act, the Chinese anti-bribery laws, and other applicable laws and other global requirements. Under these laws and Teradata policy, we must not offer, give, solicit, or receive any form of bribe or kickback to anyone, nor may we engage a third-party agent to do so on our behalf.

A bribe means giving, offering, or promising anything of value to gain an improper business advantage. A bribe does not have to be cash. Inappropriate gifts, entertainment, or

paying an inflated price to purchase property or services can also be considered bribery. A kickback is the return of a sum already paid or due to be paid as a reward for making or fostering business arrangements.

Consequences for violations of the FCPA and other anti-corruption and anti-bribery laws are severe, including fines to the individuals making or receiving the payments and the company, as well as potential prison sentences. While the FCPA specifically applies to dealings with non-U.S. governmental officials, Teradata prohibits bribery in all business dealings. The same rules against bribery that apply to activities with U.S. and foreign government officials also apply to dealings with non-governmental customers and business partners.

To stay compliant with anti-corruption and anti-bribery laws, special rules must be observed before anything of value is provided to a government employee. Note that some customers or Teradata partners are owned in whole or in part by a governmental entity. As a result, the directors, managers, employees, contractors, and other representatives of those businesses may be considered government officials. In these situations, ordinary and reasonable business entertainment or gifts typically are allowed when they are customary and legal in the applicable community, provided they comply with Teradata policies.



For more information on monetary thresholds, pre-approval requirements, and other considerations, please see the Teradata Gift and Entertainment Policy ([CMP 912](#)), the section below (“Gifts and entertainment”), or consult the Teradata Law Organization before acting.

In some countries outside the U.S., facilitating payments to low-level government officials may be permitted under local law or business customs. Facilitating payments (sometimes called “grease” payments) are small payments, typically made in cash, to expedite the performance of routine governmental administrative actions, such as the processing of paperwork or granting of a permit. However, it can be difficult to tell when a facilitating payment crosses the line and becomes a bribe. For your protection and the protection of the company, Teradata prohibits all facilitating payments. You must immediately report all solicitations of facilitating payments, as well as solicitations of bribes or kickbacks, to the Teradata Law Organization.

Teradata’s Global Anti-Corruption Policy ([CMP 904](#)) expresses a zero tolerance for bribery, corruption, and money laundering. All Teradata people must comply with this policy.

Teradata has also adopted various processes, tools, and controls related to third-party due diligence. These are intended to help screen out and prevent dealings with third parties who are known to be involved in corrupt activity. They also help ensure high-risk or red-flagged third-party dealings are implemented in compliance with all applicable legal requirements and with due consideration of reputation risks. All Teradata people must comply with these processes and tools.



Anti-corruption guidance

Question: An official with a non-U.S. telecommunications company or bank that is partially government owned tells you Teradata will get favorable treatment in a pending business opportunity if Teradata will: hire the official’s son; award a subcontract to the official’s brother’s company; provide a charitable donation to a scholarship fund that benefits the official’s niece; or cover the expenses for the official’s family to accompany him on an otherwise legitimate business trip. What should you do?

Answer: You should decline the request and immediately report it to your manager and the Teradata Law Organization. You and/or your manager should also immediately report it to the Teradata Ethics & Compliance Office. The U.S. Foreign Corrupt Practices Act (FCPA) applies to U.S.-based companies and all their subsidiaries globally that deal with officials of non-U.S. state-owned enterprises, such as the telecommunications company or bank involved in this scenario. Trading, soliciting, or offering favorable treatment in business dealings with such officials in exchange for personal favors for the official or their family, whether in cash, cash equivalents, or in kind (such as providing a job, a subcontract, a charitable scholarship, or travel that benefits their family members here) is prohibited and must be immediately reported.



Export and import compliance

For Teradata to participate in the world market as a high-tech company, we must be particularly aware of international trade and immigration laws and restrictions. The export of goods and technology from most countries, including the United States, is strictly regulated. Communicating technical information to a person in another country (or to a citizen or representative of another country, even if that person is temporarily located within the same country as you) can be considered an export under the law. Whether a product or technology may be exported depends on several factors, including the nature of the item, the country of destination, and the intended end use and end user.

For more information on export activity and the laws that govern such activity, please see our Export Compliance Policy ([CMP 919](#)) or contact the Law Organization.

Teradata also must comply with all applicable import laws and regulations. These laws typically govern what can be imported into a country, how the goods must be marked, classified, and valued, and what duties or other taxes must be paid on them. The penalties for violations of both import and export regulations can be severe. If you are involved in the import process for Teradata, you should read and understand the company's Import Compliance Policy ([CMP 917](#)). For guidance about import regulations, consult your organization's designated import compliance liaison or the Teradata Law Organization.

Teradata expects each of us to comply with all applicable import and export control laws and regulations. We supplement these laws and processes with third-party due diligence tools and controls designed to prevent and reduce the risk of bribery and corruption as well as comply with trade restrictions and sanctions. We are all charged with ensuring we understand who our customers are, how our products will be used, and the end destinations of our products.

As a U.S.-based company, we are subject to restrictions on trading with some specific countries, individuals, or entities. We are also prohibited from activities related to certain other countries', groups', or customers' attempts to implement boycotts, embargoes, or other trade restrictions, if those actions are incompatible with U.S. trade policies (for example, efforts by some to restrict or prohibit trade with Israel). We keep detailed policies ([CMP 903](#) and [CMP 919](#)) and routinely updated listings (e.g., Denied Parties Listings) regarding the individuals and countries with whom we may not trade and regarding what boycott and embargo activities are prohibited. If you have any questions about trade and economic sanctions that may apply to your work, please contact the Law Organization.

Gifts and entertainment

Gifts can be anything of value, including goods, services, travel, lodging, meals, and entertainment, even when the giver is not present. Gift-giving practices vary around the world. Business gifts and entertainment are courtesies designed to build good working relationships with customers and business partners. Gifts are inappropriate, however, if they are excessive, create an obligation, or are given with an intent to improperly or corruptly influence a business decision.

Gifts are permitted generally if they are:

- Nominal in value
- Infrequent
- Provided openly
- Unsolicited
- Not cash or cash equivalents (such as a loan, stock, or gift certificate)
- Something that would be considered appropriate by an independent observer (e.g., we should not provide or pay for adult sexually oriented venues, services, or entertainment)
- Legal in the local setting in which it is given and consistent with the policies of the other company



When dealing with government customer representatives, you must be particularly cautious. Laws prohibit some government employees from receiving anything of value, even a modest lunch, a cup of coffee, or a token item, such as a meal or promotional item bearing the Teradata logo.

The standard maximum permissible threshold limit for gifts under Teradata policies (**CMP 912**) is USD \$100 for gifts and USD \$200 for entertainment. Lower limits may apply under departmental, local, or team policies, rules, or local law (for example, those involved in procurement or entertainment of government officials or representatives of enterprises that are wholly or partially government-owned). You may request management approval in advance for different amounts using the approach set out in CMP 912.

If you are offered a gift or entertainment that is not allowed or is over the amounts set forth in Teradata policies, you should politely explain that Teradata policies do not permit you to accept it. If you find yourself in a situation in which refusing such a gift would embarrass or offend the person offering it, you may accept the gift on behalf of Teradata, and then report it immediately to your manager.

You should always respect the codes of conduct and policies of other companies. If a gift or entertainment is allowed under Teradata policy but prohibited by the recipient's code or policy, you should not offer the gift. By far the most important things to remember are that you cannot offer, give, solicit, or receive anything that would compromise—or appear to compromise—the recipient's ability to make objective business decisions, and that you must make sure gifts and entertainment are transparent to management and accurately reflected and disclosed in appropriate company documentation. Even if you were to use your own money or other resources to provide a gift or entertainment to a customer representative, you still would need to comply with these requirements.

Environmental, health, and safety (EH&S)

In keeping with our commitment to an exceptional workplace, Teradata follows all applicable EH&S laws, rules, and regulations in the communities where we conduct business. We have an EH&S handbook as well as EH&S policies, standard operating procedures, mandatory reporting requirements, and mandatory training for all associates. Information concerning these is available (see **CMP 601**); much of it also is publicly accessible at **Teradata.com**.



Social responsibility and human rights

We also have proactive environmental sustainability, human rights, and other related environmental, social, and governance (ESG) initiatives, including compliance with regulations addressing hazardous content in our products; electronic waste recycling; efforts to reduce emissions where possible; product standards; conflict minerals human rights commitments; required compliance with our supplier code of conduct; and incorporation into our business of the principles of the Responsible Business Alliance [RBA] Code of Conduct and the United Nations (UN) Global Compact. Information concerning these and other programs is publicly available at <https://www.teradata.com/about-us/environmental-social-governance>.

If you have any questions, or if you become aware of an unsafe condition or a possible violation of EH&S laws, regulations, policies, standard operating procedures, or our commitments to sustainability, human rights, and other related ESG initiatives, you should immediately report it to your manager, facility manager, the Law Organization, or the Ethics & Compliance Office.

Human rights

Teradata follows the 10 principles of the United Nations Global Compact.

General

1. Support and respect the protection of internationally proclaimed human rights.
2. Make sure that we are not complicit in human rights abuses.

Labor

3. Uphold the freedom of association and the effective recognition of the right to collective bargaining.
4. Uphold the elimination of all forms of forced and compulsory labor.
5. Uphold the effective abolition of child labor.
6. Uphold the elimination of discrimination in respect of employment and occupation.

Environment

7. Support a precautionary approach to environmental challenges.
8. Undertake initiatives to promote greater environmental responsibility.
9. Encourage the development and diffusion of environmentally friendly technologies.

Anti-corruption

10. Work against corruption in all its forms, including extortion and bribery.

Pursuing innovation

Innovation and agility in execution are at the core of who we are as a company. We balance these core principles against our need to protect one of our most important assets: our proprietary information. We all must cooperate in following the rules of the road for managing Teradata's proprietary information. Our future achievements as individuals and as a company are built upon the base of our accumulated assets, knowledge, and training. It is essential that we protect Teradata's intellectual property rights. We also must understand and respect others' intellectual property rights and not violate those rights—intentionally or unintentionally.

Proprietary and confidential information

Information is a key Teradata asset. It includes our intellectual property and other protected information, such as:

- Trade secrets, other confidential information, patents, trademarks, and copyrights
- Research and development, including inventions, patent applications, and engineering records
- Network management information
- Business, marketing, and service plans
- Customer and prospective customer identities
- Pricing and other quote, proposal, and contractual terms
- Merger and acquisition candidates
- Unpublished financial plans, data, reports, and projections
- Examination/test material for the Teradata Certification Professional Program
- Information subject to written nondisclosure/confidentiality agreements

While sharing information is necessary in our interconnected workplace, we all need to protect information belonging to Teradata, keep it from being exposed to unauthorized people, and ensure it is used only for legitimate Teradata business purposes. We must likewise protect proprietary information belonging to companies with which we conduct business, such as our customers and business partners, against unauthorized disclosure and use.

Additionally, during the course of our work, some of us have access to personal information entrusted to Teradata by our fellow associates, customers, and business partners (for example, information protected under privacy laws). If your job gives you access to this type of information, you must take all reasonable precautions to ensure it is treated with care and respect and in compliance with all legal requirements. It should be used only for legitimate business purposes and only accessed by those who need to know it to do their jobs. We cannot share this information even with fellow associates or transfer it across borders without appropriate authorization. You should take precautions to label any document or email containing confidential and/or private information as Teradata Confidential Information.

Because confidential information is not always marked, if you are uncertain about whether use or disclosure is proper, review applicable Teradata policies (e.g., [CMP 1402](#) and [CMP 204](#)) regarding protecting information, and ask your manager or the Teradata Law Organization before you use or disclose the information.





Third-party intellectual property

Teradata respects the intellectual property of its vendors, suppliers, and competitors, and expects other parties to respect Teradata's intellectual property. Each Teradata associate must use only properly licensed software or other intellectual property. Our associates must not download software or other intellectual property without the knowledge or approval of the Teradata Procurement or IT teams. You should be aware that the use of stock photography, music, or open-source code or text in any Teradata-produced material, such as Microsoft PowerPoint® or other presentations, can put the company at risk. You must ensure Teradata or its vendors have the appropriate licenses and ability to use such material before it is incorporated in presentations or other media.

We may use open-source computer code, which is often freely available, in connection with Teradata intellectual property. However, the licensing terms for some open-source computer code could mean that related (or even unrelated) Teradata intellectual property might be placed in the public domain. This is particularly a concern if the open-source computer code is embedded in our products in certain ways or is not used in accordance with certain requirements that are necessary to avoid that consequence.

Teradata has adopted and applies intellectual property and open-source content policies, practices, and procedures. Associates involved in activities related to such must be familiar with and comply with them. If you have any questions about intellectual property or open-source content, contact your manager or the Teradata Law Organization.

Teradata Certification Program

Our company provides us with the resources we need to obtain professional certifications. Those taking certification exams must read and understand the Teradata Certification Security Policies before obtaining exam study material and/or taking any exams. Certification exam content (both the questions and answer options) is part of Teradata's intellectual property and is not to be shared or discussed with anyone in any manner. People or entities that copy, distribute, post, receive, download, buy, or sell our proprietary materials are violating laws, Teradata rights, and Teradata policies. Associates must refrain from engaging in any such activity. If you come across any such materials, you should report it to certification.teradata@teradata.com.

Privacy and data protection

Teradata has built a well-deserved reputation as an organization that has earned the trust and respect of our customers and Teradata associates. We must uphold that trust and respect by protecting the confidentiality, integrity, and availability of data, including personal information. Each of us must follow all relevant procedures for processing and handling confidential data, such as:

- Allowing access only by authorized persons (e.g., Teradata associates and business partners with a legal and legitimate need to know it) for legitimate Teradata business purposes and associated time periods
- Closely guarding passwords and the technology accessed with those passwords
- Resisting the instinct to be immediately helpful when unverified or unauthorized people seek access to data, funds, or approvals, such as through pre-texting or phishing attempts
- Maintaining careful backups in accordance with and otherwise complying with our data management policies and information protection standards
- Never sending confidential data of Teradata or its customers to your personal email/devices

If you become aware of a data security incident, violation, or breach, no matter how minor, you have an obligation to Teradata and our customers to report it immediately so we can address and limit any damage, make any filings or disclosures required by applicable laws, regulations, or contracts, and take steps to comply with other data and privacy protection laws and regulations as quickly and completely as possible. Ignoring a data security breach is not an option.

All of us should read, understand, and comply with the provisions of our Global Privacy Statement located at <https://www.teradata.com/Privacy>. All Teradata associates play a critical role in maintaining the highest standards of data protection. If you are in doubt about how to use personal information that you come into contact with in your work, Teradata's Privacy Office is here to help you. You can also find Privacy Office guidance [here](#).



Artificial Intelligence (AI)

AI presents all of us with tremendous opportunities and efficiencies in our work at Teradata. AI tools and technology—including generative AI—have the potential to revolutionize the way we work, make data-driven decisions, and serve our customers better. With immense potential, however, comes added responsibility.

At Teradata, we prioritize responsible use of AI to improve the quality, productivity, and overall value of our work and business outcomes. Accordingly, every Teradata employee is encouraged to exercise diligence, caution, and responsibility as well as obtain manager approval prior to using new AI tools at Teradata. You can read our Acceptable Use Policy and general guidance on how to use AI [here](#).

All uses of AI must address the following key risks:

- Ethical use
- Data privacy, governance, management
- Data security
- Security practices
- Ownership and copyright
- Content verification
- Third-party risk management
- Bias

The Law Organization is here to help you with any AI-related questions you may have.

Rising to the top of our industry

At Teradata, we are customer and market driven, another of our core principles. Although we compete aggressively, we do so fairly and with the right attitude. We follow the rules and best practices for fair competition. We strive to be world-class and best-in-class in all our market segments. At the same time, we must not forget that personal and corporate integrity are the foundations of our mission.

Competing fairly

Teradata is committed to succeeding based on merit and the quality of our products, services, people, and business partners, regardless of where we operate. We comply with laws intended to protect competition and free enterprise globally, including laws referred to as antitrust laws or fair competition laws.

Under fair competition laws, we may not make any agreement with a competitor that restricts competition. Illegal agreements do not have to be signed contracts. They might be as simple as an oral understanding between two competitors. Any coordination or collusion among competitors is serious and places both you and Teradata at risk.

When communicating with competitors, you must not raise, discuss, or address any of these matters:

- Dividing territory
- Dividing customers
- Charging customers a fixed or certain price
- Paying suppliers a fixed or certain price
- Offering the same or similar discounts, terms, or conditions of sale
- Requiring downstream resellers to charge a fixed or certain resale price
- Boycotting a particular customer or supplier
- Agreeing who will win a particular bid

If any of these topics arise when communicating with a competitor, you should stop the conversation immediately, make your disapproval as obvious as possible, and report the situation to the Teradata Law Organization immediately.





Participating in industry associations and trade shows

Industry associations, conferences, and trade shows can be wonderful networking and business development opportunities, but they can also pose legal and ethical challenges. When attending these events, be careful to avoid even the appearance of improper collusion. If you become aware of any formal or informal discussion between competitors regarding anti-competitive topics at any of these events, you should excuse yourself and contact the Law Organization.

Dealing fairly with customers

Teradata is known for its extraordinary customer dedication and service. To live up to this reputation, we must deal fairly with our customers.

Fair competition laws generally allow Teradata to choose the companies with which we conduct business. However, those decisions must be made independently and never in agreement or collusion with competitors.

As part of dealing fairly with customers and avoiding violating competition laws and fair-trade laws, you must never:

- Make false, unfounded, or misleading statements about our competitors' products or services, or make false or unfounded comparisons of their products/services with ours
- Make commitments or promises that you or Teradata do not intend to or are not able to keep
- Sell comparable goods on comparable terms at significantly different prices, during the same time periods, in the same volumes, and in the same geographies to customers who compete with one another. Significant pricing deviations for competing customers that are not justified based on objective differences in products/services, timing, geography, terms, volumes, and the like, can constitute illegal, anti-competitive price discrimination

If you have any questions about how to deal fairly with customers, seek guidance from the Law Organization before you act.

Not abusing market power

Fair competition laws also restrict companies from taking actions that discourage innovation and competition based on their market power. To avoid abusing market power, you must never:

- Sell our goods and services at below-cost pricing with the intent of driving competitors out of the market
- Tie the purchase of certain goods and services to the required purchase of additional items
- Make reciprocal deals with customers (commit to buy their products if they commit to buy ours) unless pre-approved by the Law Organization
- Make exclusive dealing arrangements without prior approval from the Law Organization

Business intelligence

Obtaining accurate information about our competitors' activities is necessary and may even be part of your job. We obtain this information ethically and from legitimate sources. These include publicly available documents, analysts, publications, and the Internet.

We may not, however, gain a competitive advantage by obtaining information through illicit means. We may never steal confidential business information or trade secrets by any means—not through bribery, espionage, false pretenses, or other illegal or unethical behavior. This means, in part, that you should not ask for or encourage others to share with you any information that would violate a confidentiality agreement they have with any other company. If someone sends you confidential information unsolicited, you should advise the Teradata Law Organization immediately.

Teradata competes fairly and aggressively but legally. If you are a former employee of a Teradata competitor, do not disclose or use any of your prior employer's confidential information or trade secrets in connection with your Teradata job. Even if you are asked by one of your colleagues or managers to share such information, you must not.



Ethics and compliance contacts and resources

Teradata Ethics Helpline

The toll-free helpline is available 24 hours per day at 866- 455-0993 (outside of the United States, callers may call toll-free through AT&T Direct) and online at www.integrity-helpline.com/tdhelp.jsp. You can make good-faith reports of suspected violations or raise ethics and compliance concerns and questions, anonymously and confidentially if you choose (where not restricted by law), and without fear of retaliation. Calls may be made in multiple languages.

Teradata Ethics & Compliance Office email inbox

Email E&C@teradata.com. You can make good-faith reports of suspected violations, raise ethics and compliance concerns and questions, confidentially if you choose, and without fear of retaliation.

Teradata Law Organization

Email Molly Treese at molly.treese@teradata.com or reach out to any other member of the Teradata Law team. Employees at Teradata can view a list of legal team contacts on the Law Hub at <https://teradata.sharepoint.com/sites/LawHub/SitePages/The-Law-Team.aspx>.

Teradata Certification Program

Email at certification.teradata@teradata.com for questions about illegal or questionable study materials, suspicious testing behavior, certification title representation, and logo usage. Please see our security and privacy [page](#).

Teradata Internal Audit

Email internalaudit.teradata@teradata.com for issues regarding financial irregularities.

Teradata Corporate Security

For issues regarding physical security or theft, contact global Corporate Security at Teradata.SAFE@teradata.com.

Teradata Information Security

For issues related to information security for Teradata products or corporate environment, contact information.security@teradata.com.

Teradata Global Policies

Employees of Teradata have access to our Global Policies website at <https://teradata.sharepoint.com/teams/policy>, where each of the policies referenced in the Code can be found.

Teradata.com and other online resources

Teradata.com offers information about Teradata corporate governance policies and practices (see Teradata.com/About-Us/Corporate-Governance) and about Teradata's other corporate social responsibility and sustainability policies, practices, and initiatives (see Teradata.com/About-Us/Corporate-Social-Responsibility). Employees of Teradata also have access to our Ethics & Compliance Sharepoint site at <https://teradata.sharepoint.com/sites/LawHub/SitePages/Ethics-&-Compliance.aspx> which contains reference guides, training videos, and other information on each of the topics addressed in the Code.