Global Code of Conduct

The Code Connects Us All

Section One:
The Code

A Letter From Our Executive Chairman and CEO

Dear Colleague,

Thank you for taking the time to review our Code of Conduct.
As employees of Tech Data, we all have a responsibility to know and put into practice the principles and standards that make our company a highly respected, reputable and trusted industry leader.

Tech Data was built on a strong foundation of shared values—principles that continue to keep us grounded in our mission and help us navigate uncharted territory in an ever-changing IT landscape. These values—integrity, excellence, accountability, collaboration and inclusion— serve as the cornerstone of our culture, giving us a shared sense of purpose as we strive to deliver the best experience possible to our channel partners and to each other.

Within Tech Data and in our communities, the actions we take are a reflection of who we are and have a tremendous impact on the reputation of our company. Our Code summarizes key elements of company policies designed to ensure lawful and ethical conduct, and clearly sets the expectations for our job-related activities so that the actions we take are the right ones.

The Code applies to all of us: Tech Data employees, officers and board members. It is designed to serve as a guide for appropriate conduct and a resource to help you make the right decisions. Please read it, know it, and when something does not seem right, speak up. Tech Data relies on you to raise questions and concerns so that we can continuously improve our processes and solve any problems that may arise.

Thank you for your continued dedication to Tech Data and for your help in protecting and strengthening our reputation for integrity and excellence.

Rich Hume, CEO

Bob Dutkowsky, Executive Chairman

OUR SHARED VALUES

Our values serve as the foundation from which we work and drive our organization forward each day with a shared sense of purpose.

- **Integrity:** We do what's right.
  Integrity is the foundation of our business. We are honest, transparent, and always do the right thing by acting with the highest standards of ethics and fairness.
- **Excellence:** We deliver excellent experiences.
  We strive to achieve the highest levels of performance in everything we do. We deliver the best experience possible to our channel partners and to each other.
- **Accountability:** We keep our promises.
  We keep our promises and deliver on our commitments. We set clear expectations, then empower and trust each other to make decisions to achieve our collective goals.
- **Collaboration:** We support each other.
  We listen to and support each other. We work together, always looking for better, more innovative ways to be agile, reduce complexity and improve our business.
- **Inclusion:** We win together.
  We believe our diverse global workforce drives our success. We provide an inclusive, welcoming and enriching environment for our colleagues and their ideas.

An Introduction to the Code

The Code is our guide for making the right business decisions based on integrity. It's a resource that provides answers and direction when facing complex and challenging situations.

Why We Have a Code

The Code reflects Tech Data's firm commitment to conducting business in alignment with our shared values, policies and applicable laws. The Code defines our expected behavior when interacting with each other, our business partners and our communities.

How the Code Applies to Me

We are all accountable for knowing the Code and speaking up when we see misconduct. Always ask yourself if your actions are consistent with our shared values. This Code cannot provide every answer, so if you are not sure about something, seek guidance.

By competing fairly and following all applicable laws, we reduce risk to our company and business partners and enhance our company's reputation for integrity.

Contents

Section 1 - The Code

A Message From Our CEO
Our Shared Values 2
An Introduction to the Code 2
Why We Have a Code 2
How the Code Applies to Me 2

Section 2 - The Connection

Who Must Follow the Code

Additional Expectations for Leaders 6
Waivers 7
The Cost of Non-Compliance 7
Non-Retaliation 8
Application to Business Partners 8
Raising a Concern 8
The Internal Process 9
Discipline for Violations 9

Section 3 - The Content

In the Workplace

Preventing Harassment and Discrimination 11
Health and Safety in the Workplace 11
Our Work Environment, Working Conditions and Human Rights 11
Protecting Information 12
Personal Information 12
Records Management 13
Intellectual Property 13
Using Tech Data IT Systems 13
Cybersecurity 14
Gifts, Travel and Entertainment 14
Conflicts of Interest 15
Accurate Books and Records 15
Financial Integrity and Reporting 16
Authority to Make Commitments on Behalf of Tech Data 16

Contents cont.

With Business Partners

Understanding and Complying With Partner Policies	17
Interaction With Our Business Partners	17
Doing Business With the Government	17

In the Marketplace

Anti-Bribery and Anti-Corruption	18
Competition and Antitrust	18
Competitive Information	19
International Trade Controls	19
Anti-Boycott and Trade Sanctions	19
Insider Trading	20
Anti-Money Laundering	21
External Inquiries	21
Social Media	21

In Our Communities

Corporate Social Responsibility	22
Political and Charitable Activities	22
Respect for the Environment - Sustainability	22

Section Two:
The Connection

Who Must Follow the Code?

The Code of Conduct applies to everyone at Tech Data. This includes our Board of Directors, executives, employees and agents acting on behalf of Tech Data around the world. We also expect our business partners to follow these same principles. The Code connects us all, ensuring consistency in the way we do business, regardless of culture or location.

Your responsibilities as an employee of Tech Data are to:

- Act with integrity, respect and professionalism.
- Make decisions that are well-founded and within the law.
- Never compromise Tech Data's reputation or your own.
- Be honest.
- Ask and speak up when you are in doubt or witness misconduct.
- Ensure compliance is part of your team culture.

Additional Expectations for Leaders

Leaders are expected to create an environment that supports a culture of compliance and open communication, where employees feel comfortable raising concerns without the fear of retaliation. All leaders are expected to:

- Follow the Code, Tech Data policies and applicable laws and regulations.
- Be available to anyone who raises a concern and take employee concerns seriously.
- Never retaliate against anyone who raises a concern and protect others from possible retaliation.
- Report suspected misconduct immediately. Never cover up or ignore misconduct or retaliation.
- Lead by example, holding yourself and others accountable, avoiding even the appearance of violating the Code or law.
- Integrate compliance into your team culture.
    - Create an environment that encourages straightforward communication around issues or concerns related to the Code or applicable laws.
    - Recognize employees that demonstrate integrity and a commitment to compliance.
    - Be proactive, identify potential weaknesses, and take corrective action when appropriate.

If Leaders fail to report known violations in our company, they may be subject to discipline, including termination. Leaders are also expected to exercise proper oversight in their areas of responsibility so they are aware of things that might create risks for our company and take action to mitigate those risks.

Tech Data adheres to all laws and regulations in the geographies where we do business. In some cases, regional policy and local laws may be stricter than the policies referenced in this Code. When this happens, you should follow the local laws and policy.

Waivers

Any waivers or exceptions to the Code must be disclosed to the applicable regional President along with the reason for the request. The request will also be reviewed by the Ethics and Compliance Department. If the waiver involves an executive officer, financial executive, or member of Tech Data's Board of Directors, only the Audit Committee of the Board of Directors can grant this waiver, which must be disclosed as required by the rules of the NASDAQ OMX exchange.

The Cost of Non-Compliance

Failing to comply with the principles of our Code can put our company's reputation at risk. For our shareholders, vendors and customers, it is important to know Tech Data is a reliable business partner. Companies with strong cultures of integrity tend to be respected in the marketplace, leading to a competitive advantage and positive business outcomes.

Did You Know That Violations of the Code:

- Are always avoidable.
- Can be disruptive to everyday business and take the focus off of serving our customers.
- Can damage Tech Data's reputation and put our company at risk.
- May result in severe fines and possible criminal prosecution.

Employees who violate the Code, Tech Data policies or the law face disciplinary action, up to and including termination of employment, even if they do not personally benefit from the violation. If a violation of law occurs, penalties may be imposed by a regulator or a court.

Speaking up Early Can:

- De-escalate a situation.
- Minimize risk and disruption to our business.
- Bring clarity and resolve potential issues in a timely manner.
- Protect victims of harassment, discrimination or other types of misconduct.

Non-Retaliation

Tech Data is committed to protecting the rights of individuals who report concerns about suspected misconduct in good faith.

Tech Data does not tolerate acts of retaliation - such as firing, demoting or harassing anyone because they submit a good faith report or participate in an investigation.

If you believe someone has retaliated against you, you should report the matter immediately.

Any act of retaliation is a violation of the Code and is grounds for discipline, up to and including termination. See the **Anti-Discrimination, Anti-Harassment, and Non-Retaliation Policy** for more information.

Reporting in "good faith" means you believe your information is accurate. It is not based on the outcome, or whether the reported behavior turns out to be unethical or illegal.

Application to Business Partners

We expect our business partners to act ethically, responsibly and in accordance with the principles established by our Code and applicable law. If you are responsible for hiring or managing a third party, it is your responsibility to ensure they have a good reputation and understand the requirements of our Code. Tech Data's **Supplier Integrity Principles** establish and communicate the fundamental requirements for being a supplier of goods or services to Tech Data.

Raising a Concern

You have a responsibility to raise concerns and ask questions. Promptly raising concerns allows our company to address problems early, before more serious consequences occur. If you have a question or concern, your immediate manager is normally the best place to start. If you are not comfortable talking with your manager or if your concern is not addressed, you should contact another member of management, Human Resources, an Ethics Advisor, the Legal Department or Tech Data's Ethics and Compliance Department **{EthicsandCompliance@techdata.com}**.

Report a concern if you observe behavior that:

- Is not legal
- Does not comply with Tech Data's policies
- Does not align with Tech Data's core values
- Would adversely affect Tech Data
- You would feel concerned reading about in a news headline

If in doubt—ask for advice.

No matter how you share a concern, Tech Data will address it promptly and make every effort to safeguard your privacy during and after the investigation. Your obligation is to tell the truth and participate in the investigation as needed.

The Internal Process

Tech Data will investigate all good faith reports and take appropriate action when necessary by following these steps:

1. Assemble a team of qualified and independent investigators.
2. Gather facts and conduct interviews.
3. Keep the appropriate level of management informed throughout the process and help them determine the next steps based on facts.
4. Communicate regularly with the person who reported the concern.

Discipline for Violations

All employees are responsible for knowing the Code and company policies. Employees and business partners must comply with applicable laws and regulations in the countries where they do business. Violations of the Code, company policies or the law may carry serious consequences for individuals and Tech Data, such as damage to our reputation, fines and possible civil or criminal liability. Employees engaging in unethical or illegal behavior will be subject to disciplinary action, up to and including termination. Tech Data will refer cases to government authorities when appropriate.

The Tech Data Ethics Line is available online and over the phone 24 hours per day, seven days a week, around the world. Employees in most countries can choose to remain anonymous when reporting through the Ethics Line. However, please be aware that remaining anonymous may hinder Tech Data's ability to resolve your concerns if you can't be reached for follow-up questions. To raise a concern online or to find a list of global numbers, visit **techdataethicsline.com**.

The Ethics Line is managed by an independent company not affiliated with Tech Data.

Section Three:
The Content

Preventing Harassment and Discrimination

Tech Data maintains a workplace culture that is respectful and professional at all times. Tech Data will never make decisions that are based on race, religion, color, national origin, age, gender, disability, sexual orientation, veteran status, gender identity or expression, or any other factor protected by law. Tech Data also makes all reasonable accommodations for qualified employees with disabilities.

A respectful work environment is free from intimidation, harassment and bullying. This includes any unwelcome conduct that creates an intimidating or offensive situation. Harassment may be in the form of physical actions, verbal statements or material—such as inappropriate videos, pictures or emails. Sexual harassment includes unwelcome sexual advances, lewd comments or jokes of a sexual nature. Tech Data will not tolerate harassment in any form.

If you experience or become aware of any act of discrimination or harassment, contact your manager or any of the other reporting options. For more information, refer to the ***Anti-Discrimination, Anti-Harassment and Non-Retaliation Policy****.*

Health and Safety in the Workplace

Tech Data is committed to having a workplace that is safe, healthy and non-threatening. We have a number of health and safety-related policies and procedures in place in our various locations and are committed to compliance with safety laws in all countries in which we operate. We continuously review and improve our work practices and the safe operation of our facilities. Our company prohibits the sale, purchase, use or possession of illegal drugs—or the misuse of alcohol or prescription drugs—while on company premises or conducting company business. If alcohol is offered at a company or business event, it is your responsibility to conduct yourself professionally.

Acts or threats of violence are forbidden by Tech Data. This includes aggressive or intimidating behavior and language, written or verbal, regardless of the intent.

Our Work Environment, Working Conditions and Human Rights

Tech Data operates around the world, and we embrace the diversity of our workforce. We are committed to the fair and equitable treatment of all people and prohibit harsh or inhumane treatment of any employee. We comply with the employment laws in all countries where we operate. Tech Data follows all applicable wage and hour laws, including minimum wage, overtime and maximum hour rules. Employment must be freely chosen. Human trafficking, forced, bonded, or involuntary labor is forbidden, as is the exploitation of children and child labor. The company also fully respects our employees' right to freedom of association.

Freedom of association

Tech Data recognizes the rights of its employees to freely associate with groups of their choosing, to bargain collectively and to share ideas or concerns with management regarding working conditions or management practices. In the workplace this generally means that employees have the right to choose to join a union. Tech Data does not tolerate discrimination, harassment or retaliation against anyone that exercises their right to join a union.

Protecting Information

Our employees and business partners trust us with some of their most important information. We are committed to treating that information with care and to respecting reasonable privacy expectations of our colleagues and business partners.

Confidential information should only be shared with fellow employees who are authorized and have a legitimate business need to know. You must protect all confidential information that is in your possession.

Unless you are authorized, you must not reveal confidential information to anyone outside Tech Data. If you are authorized to share confidential information with a third party and have a legitimate business need, you must have a properly executed nondisclosure agreement in place prior to any confidential discussions. Do not sign another company's nondisclosure agreement or accept changes to our standard nondisclosure agreements without approval from the Legal Department. See the **Worldwide Disclosure Policy** for more information.

- Do not discuss confidential information in any public areas or places where you can be overheard.
- Do not leave confidential information unattended at any time.
- Never post Tech Data's confidential information on external websites, including social media.

Confidential information refers to anything that is not in the public domain, and may include but is not limited to: trade secrets, financial results, pricing plans, customer lists, sales figures and strategic documents.

Personal Information

We collect and retain certain confidential personal information that is necessary to conduct our business and help our company operate effectively.

Personal information like phone numbers, names, email addresses and other information may be subject to special rules. You must respect and safeguard the confidentiality of this information and not access, share or otherwise use these records unless there is a legitimate business need and it is in accordance with local laws.

Confidential personal information may include, but is not limited to:

- Disabilities, personal health issues or medical procedures
- Compensation and performance reviews
- Contact information, such as home addresses and telephone numbers

Records Management

A business record is any document, including electronically stored information, that relates to Tech Data's business operations. It is your responsibility to ensure that records are retained in accordance with the **Tech Data Records Management Policy** and Retention Schedule, which outlines the period of time that records must be retained to satisfy legal and regulatory requirements. Records may be stored in hardcopy or electronic format, and must be protected, legible and retrievable at all times. When a record has met its retention requirements, it should be permanently deleted or destroyed.

Certain records may be identified as being relevant to an investigation, audit or litigation. At that time, you may receive a 'legal hold' from the Legal Department with instructions to keep certain documents (in paper or electronic form). This means that under no circumstances should any documents related to the legal hold be deleted, altered or destroyed. Failure to comply with a legal hold may result in disciplinary action, as permissible by law. In addition, never falsify or inappropriately modify business records. Doing so is not only unethical, it may also be a crime.

Intellectual Property

It is our obligation to protect Tech Data's assets and enforce our company's intellectual property rights (IP). To the extent permitted by law, our company owns the rights to all IP that is created by Tech Data employees if it is related to the company's business.

We must also respect the IP that belongs to other companies. Be especially cautious when using another company's name or logo, as this could infringe that company's intellectual property rights. We uphold all licensing agreements belonging to third parties when operating software programs on a company computer or other IT resource. Only software properly licensed by Tech Data is permitted to be used for business reasons.

Using Tech Data IT Systems

You must use any equipment provided by Tech Data responsibly. While Tech Data allows personal use of company-supplied technologies in certain circumstances, you must exercise professionalism and common sense when using Tech Data's IT resources for personal purposes. You may not download unlicensed software or copyrighted materials. Be prudent when sending electronic messages, including email, instant messages and text messages. These communications are permanent and can be forwarded without your permission or knowledge.

We may never use company IT resources to perform illegal or unethical activities, such as downloading inappropriate material, or anything that could be considered obscene, pornographic, indecent or offensive. Tech Data may monitor and restrict the use of its IT resources to the extent allowed by law. For further guidance, please consult Tech Data's IT Security Policies.

If you bring your own equipment to the office or use private equipment for business use, it is your responsibility to ensure you comply with all applicable policies.

Cybersecurity

Tech Data could be harmed by cyber risks including fraud, ransom and information theft, which could impact the financial health and the reputation of the company. Cybercriminals leverage an increasingly sophisticated arsenal of tools and methods to perform their attacks, including targeted phishing, ransomware and distributed denial-of-service.

While Tech Data is constantly improving our technical countermeasures, every employee needs to adhere to important rules while working in our connected world:

- Understand and abide by the rules defined in the **Cybersecurity & Acceptable Use Policy**.
- Use passwords that are strong, secret and different for each application.
- Keep your digital identities separate between your work and personal life.
- Exercise reasonable due care when responding to unsolicited messages to avoid falling for phishing attacks, giving away sensitive information or opening attachments. Always verify that internal communication is genuine by looking for the digital signature ribbon.
- When asked to perform wire transfers, you must exercise due care by reviewing all supporting documentation and must seek additional clarification from personally known counterparties if anything looks suspicious or unusual.
- Never store confidential corporate information on systems not managed and controlled by Tech Data or in the cloud, without appropriate approvals from the IT Security team.
- Actively participate in the Security Awareness Program.

Gifts, Travel and Entertainment

Gifts, travel and entertainment provided to or received from business partners - which includes trips, events, services, meals, benefits and other things of value - must always be reasonable. Before any gifts are provided or received, you should determine if this is acceptable under our Gifts Policy. You are prohibited from providing, offering or receiving gifts, travel or entertainment that inappropriately influences business decisions or is provided to gain an unfair advantage.

*Tech Data employees may never solicit gifts, travel or entertainment. For further information, please refer to our **Gifts Policy**.*

Exchanging gifts with business partners is allowed as long as they are:

- Infrequent.
- Have no obligations or expectations attached.
- Within the limits defined in Tech Data's Gifts Policy.
- Allowed under the recipients' business gift policies.
- Not offensive, lewd or illegal.
- Not given immediately before, during or immediately after a tender or competitive bidding process.
- Not cash or cash equivalents, such as gift cards, loans or securities.

Rules related to gifts, travel and entertainment for government officials are much stricter than those set forth here. Refer to the "Doing Business With the Government" section of this Code for additional information.

Conflicts of Interest

Tech Data prohibits conduct that creates an actual or potential conflict of interest that interferes with your ability to act or make decisions impartially and in the best interests of our company. Be aware that even the perception of a conflict could create an issue. You are required to report conflicts of interest following the process outlined in our **Conflicts of Interest Policy**. Having a conflict of interest is not necessarily a violation of our Code and Policy - but failing to disclose it is.

Financial Investments or Interests

Financial investments or interests with other companies or individuals related to your work at Tech Data must not result in unusual gains for those third parties, for you or for other employees.

Personal Relationships

Personal relationships with others can lead to conflicts of interest, in circumstances where either person in the relationship could receive or give an unfair advantage or preferential treatment related to our business because of the relationship.

Outside Employment

While working for Tech Data, you may not work for any competitor, customer or vendor. Any outside job or other activity—including self-employment—may not affect your job performance at Tech Data or compete with Tech Data's interests.

Board Memberships

You may not serve as a director or in a similar governance position for any for-profit entity without the approval of a Tech Data leader at or above the Vice President level. Executive Officers may not serve on the board of directors of any for-profit entity without the prior approval of Tech Data's Chief Executive Officer.

You do not need Tech Data's approval to serve in governance positions for non-profit, community, charitable, or social organizations—provided your service does not conflict with Tech Data's best interests.

Accurate Books and Records

As a publicly traded company, Tech Data has a responsibility to its shareholders. All of our transactions, including revenue, expenses, marketing funds and rebates must be accurate and complete in our books and records and reflect the real purposes of such transactions in accordance with all applicable laws.

We must complete transactions only as authorized by management, and only use company funds for authorized business purposes. False or misleading entries in our books and records are strictly prohibited. Tech Data maintains and adheres to internal controls to ensure these requirements are met. If you are aware of or suspect a violation of our accounting or auditing standards, you must report it immediately through one of the various reporting mechanisms. **Report a Concern**.

The principal financial officers and employees working in the Finance Department have a special responsibility to ensure our financial disclosures and accounting are complete, fair, accurate, timely and understandable. Employees in the Finance Department must understand and comply with Generally Accepted Accounting Principles (GAAP), as well as all other standards, laws and regulations that apply to our company.

Red Flags

Requests to backdate transactions or contracts.

Transactions or deals that are “off the books.”

Transactions designed to hide the real underlying purposes (for example, falsifying invoices to cover up the payment of a bribe).

Financial Integrity and Reporting

Financial reporting must be honest, complete and timely. All books, records and accounts must accurately reflect financial transactions and events and conform with GAAP standards, regulations and Tech Data’s internal controls. Any falsification, concealment, misstatement, omission or alteration of any document or record is prohibited. Any public disclosure must be complete, fair, accurate, timely and understandable and done in accordance with our **Worldwide Disclosure Policy**.

All of Tech Data’s assets must be protected against misuse, loss, fraud, money laundering and theft. Appropriate care must be exercised when overseeing the use of Tech Data’s assets and when approving new customers and vendors, as well as transactions with existing customers and vendors.

Proper accounting for revenue and revenue recognition, inventory cutoff and vendor and customer rebates should be performed and accounted for in accordance with the company’s Uniform Accounting Principles (UAP). The UAP should be utilized for these sensitive topics as well as other accounting-related inquiries to ensure uniform and appropriate treatment of accounting topics. When you need further clarification, you should contact the Technical Accounting Group within Corporate Accounting.

Authority to Make Commitments on Behalf of Tech Data

To make sure all of our contracts are in Tech Data’s best interest, contract and payment approval is delegated to certain employees. If you are authorized to sign agreements or make commitments on behalf of the company, you have a responsibility to adhere to the proper approval and authorization processes before you agree to any contract on Tech Data’s behalf. This applies to oral and written agreements, as well as to any business commitments or other obligations you may arrange for our company.

Understanding and Complying With Partner Policies

The trusted relationships we have established with our business partners are vital to the success of our company. It is your responsibility to read and understand their applicable policies before initiating any transaction or operation. Do not assume your personal contact with the partner is actually an authorized representative who can approve changes or exceptions to such policies on behalf of the partner. We must be transparent and clear when working with our business partners and must not engage in operations, transactions or practices that do not comply with the policies of our partners.

Many of our business partners have specific policies and procedures applicable to transacting business with Tech Data. These policies often address such topics as special pricing, promotions or discounts, as well as the use of marketing development funds. Your responsibility is to make sure the use of special pricing, promotions, discounts and marketing development funds are for legitimate business purposes and are applied for the stated business purpose. Please refer to the **Global Marketing Development and Vendor Marketing Funds Policy** for more information.

Tech Data is committed to purchasing products directly from the original manufacturer whenever possible and to selling products directly to resellers. However, in very limited circumstances it may be necessary to acquire products from other sources or sell products to sub-distributors. Please refer to the ***Non-OEM and Sub-Distributor Policy*** *for more information.*

Interaction With Our Business Partners

It is important to Tech Data that our relationships with business partners are respectful and honest. These relationships are based on lawful, efficient and fair practices. Tech Data will not engage in unfair, deceptive or misleading practices, even if directly or indirectly requested by a partner.

Doing Business With the Government

Doing business with the government differs from doing business with other partners. Special rules may apply to hiring current or recently retired government officials, their families, and to any conduct that could seem to improperly influence objective decision making.

All billings to the government or government contractors must be truthful, accurate and conform to all pertinent laws and regulations. Contracts with the government must be strictly followed. Do not deviate from contract specifications involving products, components, testing or other items without prior written authorization from the government agency or government contractor.

A company may be considered to be a government-owned company even if the government does not own more than 50% of a company, controls the company through law, or has the ability to appoint senior management. It can be difficult to determine if someone is a government official, so ask questions and consult your manager, the Legal Department, or the Ethics and Compliance Department if you are unsure.

Anti-Bribery and Anti-Corruption

We comply with all applicable anti-corruption laws, such as the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act. Even though the FCPA is a U.S. law, it applies to Tech Data everywhere we do business.

These laws prohibit giving or offering or promising to give anything of value to government officials or private individuals in order to obtain or retain business or to gain an improper advantage. A bribe can also include non-tangible items such as offers of employment, confidential information or favors.

Tech Data does not tolerate any form of bribery. We cannot make improper payments on our company's behalf or engage an agent, or any other type of third party, to make an improper payment for us, nor can we accept bribes of any kind.

Penalties for bribing government officials are very severe.

- A bribe can be anything of value, including cash payments, charitable donations, loans, travel expenses, gifts and entertainment. In short, any payment or anything of value given with the purpose or intent to obtain an unfair business advantage is a bribe.
- Examples of Government officials include national or local government officers or employees, representatives of state-owned or controlled companies, members of political parties, party officials, former or current elected officials, candidates for political office or employees of public international organizations.
- State-owned or controlled companies also include for example public universities or hospitals.
- Facilitation payments are also prohibited under our Anti-Bribery and Anti-Corruption Policy.

For more information consult Tech Data's ***Anti-Bribery and Anti-Corruption Policy.***

Competition and Antitrust

Tech Data believes in fair and legal competition, and we abide by competition and antitrust laws everywhere we operate. These laws prohibit agreements and practices that improperly restrict or distort competition. Violations can carry serious consequences for Tech Data and for you, including corporate or personal fines, and even criminal sanctions in certain countries.

Common types of anti-competitive (and illegal) activities include:

- Price-fixing, in which competitors agree on the prices they will offer in order to manipulate the market.
- Agreeing with a competitor to divide customers or territories.

Certain agreements with competitors are almost always illegal, such as agreements to fix prices, bid rigging, the allocation of customers and territories, and the exchange of commercially sensitive information. If a competitor attempts to engage you in conversation about anti-competitive behavior, stop the conversation, and report the incident to the Legal Department immediately. Any agreements with competitors must be reviewed by the Legal Department.

It is also important to exercise caution when working with vendors and customers. Restrictions on resale prices and divisions of customers or territories are potentially illegal. Always make independent business decisions. You should never agree with a business partner about a minimum or maximum price for our products, or set a price at which a customer must resell a product, without consulting the Legal Department.

*For more information, consult Tech Data's **Antitrust and Competition Law Policy**.*

Competitive Information

Keeping up to date with information about our competitors and the market helps us to compete effectively. However, we must only gather competitive information in a manner that is legal. We want to win fairly. Never obtain information about competitors using misrepresentation, deceit or false pretense. We respect the obligations of new employees not to disclose confidential information about their previous employers. We may never misrepresent our identity when collecting information about a competitor, nor may we try to persuade another person to breach a confidentiality agreement.

> Job interviews with competitor employees are not an appropriate way to obtain competitive information. It is common to find that interviewees for open positions at Tech Data are working with our competitors. In this sort of situation, take special care to avoid the perception that you are asking for competitive information

*For more information, consult the **Antitrust and Competition Law Policy**.*

International Trade Controls

As a global company, we must comply with all regulations that apply to international trade, such as regulations on the import, export and re-export of goods and technology. Failing to do so could threaten our ability to continue to conduct business internationally, and could result in fines, penalties and even criminal prosecution. Generally, exports are products, services, technology or information shipped to a person or company in another country. In addition to referring to the physical transfer of goods, "exporting" can include activities such as traveling abroad with company information, downloading software or the release of source code and technical specifications.

Imports are goods purchased from an external source and brought into another country. Import activities are subject to laws, regulations and possible duties and taxes.

If you have reason to believe a particular transaction or shipment violates laws or internal procedures, or if you need more information about how these requirements apply to your work, consult your manager, the Regulatory Compliance Department or your local Regulatory Compliance Leader.

Anti-Boycott and Trade Sanctions

In addition to export and import laws, Tech Data must also adhere to trade sanctions imposed by the United States and other countries that restrict or prohibit business activities with certain countries or individuals who live in or originate from those countries.

As our company and many of our vendors are based in the U.S., we must follow U.S. laws and regulations that prohibit us from cooperating with requests to participate in boycotts or other restrictive trade practices the U.S. does not support. Our company cannot take any action or make any declaration that could be viewed as cooperating with an illegal boycott. These laws extend to foreign subsidiaries of U.S. companies, and apply regardless of the location where we conduct business.

Boycott requests may be subtle and can be difficult to identify. They occur when one person, group or country refuses to do business with certain people or countries as a means of protest, an expression of disfavor or a method of coercion.

*For more information, consult **Tech Data's Anti-Boycott Policy**.*

Insider Trading

As an employee of Tech Data, you may have access to "inside" information regarding our company or other publicly traded companies with which we do business. Inside information is both material — meaning it would influence a reasonable investor to buy, sell or hold stock — and nonpublic — which means it is not generally known to the trading public. Information is usually considered non-public until two full trading days have passed from the day the information appeared in the public domain.

Having inside information gives you an unfair advantage in personally buying or selling stocks. Therefore, you may never buy or sell our company's stock if you are in possession of inside information, even if your decision to trade is unrelated to this inside information. Similarly, you may not use inside information about a business partner to trade in their respective stock.

Engaging in insider trading violates our company's policy, the securities laws of the United States and the laws of many other countries where we do business. Violations of these laws can carry civil and criminal penalties for those involved. Failure to comply with this policy will also subject the individuals involved to disciplinary action, up to, and including, termination.

The following are common examples of inside information:

- Awareness of a pending or proposed merger, acquisition or divestiture.
- Knowledge of a significant sale of assets.
- Declaration of a stock split or offering of additional securities.
- Changes in senior management.
- Significant new products, customers or vendors.

How you can protect the company's information:

- Do not disclose inside information to anyone outside of Tech Data, including family members or friends.
- Avoid discussing inside information with colleagues unless doing so is necessary for business reasons.

*If you need more information or have any questions as to whether the information you possess qualifies as inside information, consult **Tech Data's Insider Trading Policy**.*

Anti-Money Laundering

The term money laundering is used to describe the process whereby individuals or organizations try to make illegal funds look legitimate or conceal them. Such individuals or organizations may also use others to make payments to circumvent tax laws or other laws. Tech Data is committed to complying with anti-money laundering and anti-terrorism laws. Penalties for violations include large civil and criminal fines.

Examples of indications of potential money laundering:

- Requests to pay more than the applicable or agreed upon price
- Payments from an unusual account
- Requests to make payments in other currencies
- Requests to pay in cash
- Payments from a third party who is not related to the account

For more information regarding our Cash Compliance, Anti-Money Laundering program, and Anti-Terrorism programs, contact Regulatory Compliance.

External Inquiries

In order to protect our name and brand, only authorized individuals are allowed to speak with external parties on behalf of our company. Inquiries from the media or investors regarding business activities, results, plans or public policy positions should be referred to the Investor Relations & Corporate Communication Department or the Department that is responsible for public relations in your country or region. In addition, Tech Data employees may not provide endorsements of other companies or products without appropriate authorization.

Sometimes we may receive requests from a governmental authority regarding our business. If you receive any such request for information, please contact the Legal Department immediately. Do not remove, destroy or alter any documents, data or records that may be relevant to the inquiry by the government.

Social Media

Personal use of social media can have an unintended impact on our company. Your communications can be interpreted as official Tech Data statements if you discuss Tech Data or our business partners on social media. Only designated employees are authorized to represent our company on any form of social media.

Employees are expected to adhere to **Tech Data's Social Media Policy** and to conduct themselves professionally when using any type of social media. You are prohibited from using company resources to transmit harassing, abusive, offensive, obscene or illegal materials.

In Our Communities

Corporate Social Responsibility

Tech Data is committed to being a responsible corporate citizen. From charitable giving and volunteerism to "green" initiatives, we recognize our responsibility to make a positive impact in the communities in which our employees live and work, and to inspire our employees to do so as well.

Political and Charitable Activities

Tech Data believes in contributing to and supporting the communities where we work. When volunteering, you must use your own time, unless you have prior approval from your manager. Company charitable donations need to be properly approved and documented and allowed under local laws, practices, and company policies.

> Donations made through charitable organizations are sometimes used to mask bribes. You should always make sure any donations Tech Data makes are not being given for improper reasons or in violation of anti-corruption laws.

Tech Data generally does not permit the use of any company funds or assets, including facilities, equipment or trademarks for political campaigns or candidates. Also, you may not use our company's name while taking part in political activities without prior authorization.

Respect for the Environment - Sustainability

Tech Data recognizes that a healthy and sustainable environment is critical to our society, economy, business and people. We strive to comply with all applicable environmental laws and regulations. We believe that our business should be conducted in a manner that embraces sustainability, recycling, and the use of renewable resources. We are committed to being a leader in developing best practices in these areas for the technology distribution market.

Tech Data