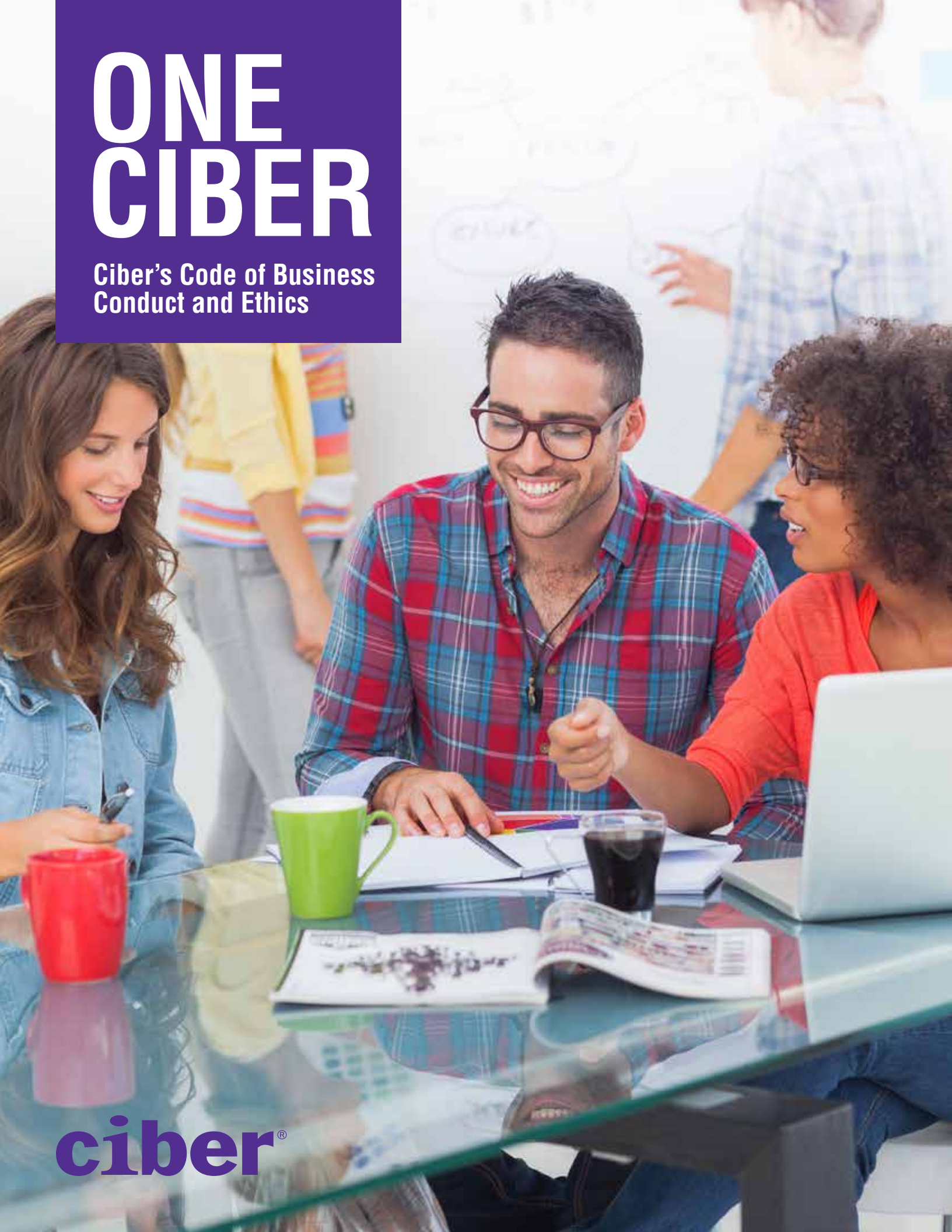
ONE CIBER

Ciber's Code of Business Conduct and Ethics



ciber®

Table of Contents

Our Commitment to Ethics and Compliance

Tone at the Top

Dear Valued Employee,

One of my most important roles is to help create the best possible work environment for everyone in our company. Enjoying our jobs is an obvious result. We should also have the comfort of knowing that we work in a safe, secure, and ethical workplace. My hope is that we are proud to work here, feel good about our jobs, and attain our highest productivity.

Every person, regardless of position, shares in the responsibility for promoting a positive environment. The Code of Conduct is all inclusive from the Board down.

Your input is essential to ensuring that we maintain a positive, productive workplace.

At Ciber, doing things the right way is an important part of who we are, how we maintain a positive, productive workplace and how we succeed in business.

We are one Ciber, constantly accelerating the pace at which we do business, and installing discipline in everything we do. We are focused strictly on discipline, process and pace.

That's why our compliance program is a critical factor for our success.

If you ever feel you can't express concerns to members of your team, you can make a report anonymously by phone using the toll-free Hotline or on the Internet at www.Ciber.EthicsPoint.com. We will protect you from retaliation when you make a report in good faith.

Together, we can achieve our mission to be One Ciber. Together, through our continued commitment to the values in this Code, we will continue to build a successful future for us all.

Thank You and Kind Regards,

Michael Boustridge
CEO

We believe that in doing the right thing every day, together we can do what's right for our clients, Ciber, and… you!

Our Values

Respect

Our behaviors should create positive experiences for the people who interact with us, including our colleagues, customers, shareholders, and partners. We should support and enforce the communities where we do business. We treat everyone with the highest degree of dignity, equality and trust. We never act in a manner that could be perceived as threatening, intolerant, or discriminatory.

Teamwork

The best solutions come from working together. We work together to meet common goals while striving to achieve excellence in all we do, creating company, team and individual professional success.

Accountability

We identify and accept our individual and team responsibilities. We hold each other accountable, not just for the results we commit to, but the experience we desire people to have. We make clear our commitments and meet them. We take responsibility for our performance in all of our decisions and actions.

Integrity

Integrity is at the core of our business. We take extra effort to promote trust and transparency in everything we do. We employ the highest ethical standards, demonstrating honesty and fairness in every action that we take. We strive for doing what is right even when no one else is looking.

Introduction

At Ciber, we believe good ethics are the basis for good business practices and will produce the best results for our shareholders. Ciber's Code of Business Conduct and Ethics contains the ethical principles that guide our behavior and are required to meet ethical and legal standards for our business. All Ciber personnel are expected to read, understand, support and practice the policies in this Code. They apply to all employees, officers and directors of Ciber. This Code supplements policies and procedures found on Ciber's internal website.

We conduct business across the world, and that means employees may be subject to the laws of different countries and organizations. We all have an important responsibility to know and follow the laws that apply wherever we work.

Our company is organized and listed in the United States. For this reason and others, U.S. law may apply even when business activities are conducted outside the United States. As a global business, we do respect and follow the laws of each jurisdiction just as other countries may apply their laws outside their boundaries as well.

Since our independent contractors and subcontractors represent Ciber in their business dealings, they must also demonstrate our commitment to ethical standards by complying with our policies. Ciber employees are responsible for educating the independent contractors and subcontractors about our policies. In addition they must meet the requirements of Ciber's Code of Business Conduct and Ethics.

We will review and revise our Code and policies as necessary to meet the changing needs of the business. Although the company will make a reasonable effort to notify employees of changes, the policies may change with or without advance notice.

Our Code of Business Conduct and Ethics

Ciber's Code of Business Conduct and Ethics reflects our commitment to doing the right thing. It brings to life our values, principles and expectations for how we do business — to always do what is right regardless of business pressures.

The Code applies to all of us, employees, officers, directors, and violations at any level are not tolerated. Managers have an added responsibility to lead by example and ensure our Code is followed by the teams they supervise while fostering a work environment that encourages colleagues to raise ethical concerns without fear of retaliation

The Code is always available through Ciber's internal website and Ciber.com, so you can review it whenever you are faced with a situation where you need more information on how to proceed.

However, the Code does not cover every situation you might encounter. It is not a substitute for good judgment and common sense. You need to understand the basic principles and standards in the Code and apply them in your work. You're also encouraged to have open and direct conversations with your manager, or talk to your HR Manager, so we can stay focused on doing the right things.

Compliance with Our Code of Business Conduct and Ethics

We believe strongly in ethical behavior across all levels of the organization, including board members, officers, and employees. We encourage you to comply with the spirit and policies in this Code. People who work together for a common purpose benefit from being aware of the guidelines. Violations of the Code should be promptly reported to the Ciber Legal Department, to your manager or HR supervisor, or to the EthicsPoint hotline.

The following list is based on the requirements of this Code and includes some, but not all, inappropriate employee conduct that could result in disciplinary action.
Engaging in practices that are inconsistent with this Code or other ordinary and reasonable rules of conduct necessary for the welfare of Ciber and our employees
Insubordination or refusal to comply with instructions or failure to perform appropriately assigned duties
Falsification of company records
Theft, fraud, carrying weapons, explosives or violation of criminal laws on company premises
Threatening, intimidating, coercing, using abusive language or otherwise interfering with the performance of fellow employees
Conduct that may endanger the well-being of any employee
Use of company materials, time or equipment for unauthorized purposes
Taking advantage of business opportunities that reasonably should be Ciber's
Misuse of Ciber's or our client's confidential information
Willful or repeated violation of our rules
Violation of client policies

Employees who do not comply with this Code or other Ciber or client policies or procedures will be subject to corrective action. Discipline can include a broad range of actions, from informal counseling to termination of employment. Disciplinary action may also include legal action and referral to a government agency, and is structured on a case-by-case basis.

We expect all of us to maintain high ethical standards, conduct Ciber business with integrity, and work in compliance with Ciber policies and the law.

- Read, understand, and comply with the Code of Business Conduct and Ethics and the Ciber policies, laws, and regulations applicable to your job.
- If you are uncertain about how to proceed in a situation obtain guidance for resolving a business practice or compliance concern.
- Report possible violations of the Code of Business Conduct and Ethics, policies, and legal and regulatory requirements.
- Be truthful and cooperate fully in any investigations.
- Complete training on the Code of Business Conduct and Ethics.
- Attest to your understanding of and commitment to the Code of Business Conduct and Ethics.

Failure to read or attest to the Code of Business Conduct and Ethics does not excuse you from responsibility to comply with the Standards, policies, and regulations applicable to your job.

Ethical Decision Making

Everyone may encounter a situation where you are unsure of the right course of action. If you encounter such a situation, ask yourself the following questions:

- Is it legal?
- Is it consistent with Ciber values, the Code of Conduct, and Ciber policies?
- Would others think it was ok if they read it in a news story?

If you can answer "Yes" to all of these questions you are likely heading down the right path. If you answer "No" or are not sure of an answer, clarify whether or not you should take the action, seek guidance before proceeding.

Remember, even if an action is technically legal but appears unethical, you should consider taking a different path.

ANSWER = ACTION
No = Do not do it
Not sure = Check it
Yes = OK

Open Door Policy/ Ethics Compliance

All of us have a responsibility to maintain and advance the business ethics reputation of Ciber and our employees. It is our management's obligation to establish and maintain processes to prevent, detect, report, and correct violations, and to make all appropriate disclosures to others with an interest in the ethical performance of the company. We all have parallel responsibilities to act in compliance with the Code and to maintain high business ethics standards and a work environment of trust and respect.

We believe that open communication is essential to a successful, ethical work environment. You should feel free to raise issues of concern without fear of reprisal. We have an "open door" policy at Ciber allowing access to any level of management including the CEO. Even when we disagree with one another, we know that healthy debate is important. We keep the communications channels open.

When communication takes the form of a concern or complaint, the best place to start is usually with your manager.

If the complaint involves your manager, or if your manager cannot solve the issue, you may take the matter to higher management within Ciber, other appropriate persons within Ciber, or to the Ethics Hotline without fear of reprisal or retaliation. Although we cannot guarantee that every concern or complaint will be resolved to your satisfaction, all complaints will be investigated thoroughly, promptly and consistently, without bias or judgment, regardless of the manner in which they are reported or the individuals involved. To the extent possible, we will keep complaints and their resolution confidential.

- You should be able to get any concern to your manager.
- Use the Open Door policy to communicate any concern to any Ciber leader.
- Ciber's Ethics Hotline is available 24/7.
- Non-retaliation means just that – no retaliation for any valid report or concern.

Employees are expected to cooperate in company investigations and answer questions truthfully to the best of their ability. You should not undertake investigations on your own. If you believe a potential violation of a policy or the law occurred, please contact either the General Counsel in the Legal Department or the Vice President of Human Resources.

Where an audit or investigation reveals the need to take corrective measures, you have an obligation to cooperate. This may include implementing changes in the systems, practices or procedures to avoid future ethics problems. However, it is a management obligation to determine, based on the facts and circumstances of each case, whether a report warrants disciplinary action. Such action may involve penalties up to and including termination of employment.

Disciplinary action, or lack thereof, does not preclude criminal or civil action by government agencies or law enforcement authorities for suspected ethics violations that may also breach applicable laws.

Complaint Procedure

Our complaint procedure provides for an immediate, thorough, and objective investigation of any claim in violation of this policy and appropriate disciplinary action.

The complaint should be as detailed as possible, including the names of individuals involved, the names of any witnesses, direct quotations when language is relevant, and any documented evidence (notes, emails, etc.). All reported incidents will be investigated. We will immediately undertake or direct a thorough and objective investigation of the allegation. In conducting an investigation, Ciber will endeavor to communicate information only to those in a need-to-know capacity; however, Ciber cannot guarantee confidentiality.

If it is determined that a violation has occurred, Ciber will take remedial action commensurate with the circumstances, up to and including discipline of employees involved. Appropriate action will also be taken to deter any future violations.

Our company will not tolerate retaliation against any employee who in good faith reports an incident or who participates in an investigation. Applicable law also prohibits retaliation against any employee by another employee or by Ciber for reporting, filing, testifying, assisting, or participating in any investigation, proceeding, or hearing conducted by a government agency.

You can report the action verbally or in writing to the following:
Your manager
Any other Ciber manager
A functional or geographic leader
Any member of the Executive Leadership Team (ELT)
The Compliance Committee
The EthicsPoint hotline

Reporting Concerns and Non-Retaliation

Ciber's anonymous and confidential EthicsPoint hotline is located at: www.ciber.ethicspoint.com

Note: This link will redirect to a secure and anonymous website. An individual can submit a report online or find phone numbers by country through this website hosting by an independent third party.

We operate with a strong commitment to non-retaliation in any form, such as harassment, discrimination or financial penalties. We believe all employees should have the ability to report concerns or suspected violations at any level without fear of reprisal or retaliation. We will protect you from retaliation in any form when you make a report in good faith. Ciber will not knowingly permit any retaliation against any employee who reports a concern.

We offer an anonymous, state-of-the-art reporting hotline through EthicsPoint, a trusted leader in confidential hotlines worldwide. EthicsPoint is a resource you can use to report your concerns if you are not comfortable discussing them face-to-face. The hotline is available 24/7/365 in any language. EthicsPoint never uses call tracing or recording devices, and, if you wish, you may remain completely anonymous. Just call if you feel something isn't right — it is simple and effective.

When you call Ciber's anonymous EthicsPoint hotline, an operator who does not work directly for Ciber will ask you a series of questions to better understand the nature of your concern. The operator then prepares a report and forwards it to Ciber's Compliance office for review, and, if necessary, an investigation. At the end of your call, the operator will give you a unique report number, a PIN and a call-back date (if you choose to remain anonymous), after which you may follow-up on your report. Simply reference the report number and PIN when you call back.

Please understand that Ciber's EthicsPoint hotline is not a substitute for meaningful communication between you and your supervisor. If you have questions or concerns about normal operating procedures, please take these comments directly to him or her.

By following the policies and spirit outlined in this Code of Conduct, and by reporting any concerns or suspected misconduct, we can help contribute to the high ethical standards by which Ciber operates. High business integrity allows us to focus on our mission to be One Ciber.

Compliance Committee

It is the responsibility of the Compliance Committee to oversee and implement procedures to facilitate effective investigations, consistent responses, clear communication, and timely resolution of for all complaints submitted through the company's anonymous hotline system as well as any alleged violation of the Code of Business Conduct and Ethics reported to the Compliance Committee by any means. The Compliance Committee is comprised of members Compliance and Internal Audit, as well as the General Counsel, Chief Administrative Officer and Chief Financial Officer, or their delegates.

Questions and Resources

There are a number of resources available to you. It is important to contact one of the following when there is a question or concern:

- Your manager.
- Any other Ciber manager.
- Any member of the Executive Leadership Team (ELT).
- The Compliance Committee
- One of the following at the Ciber Corporate office by dialing 800-242-3799.

  - Ciber's Vice President of Human Resources.

  - Ciber's General Counsel.

- The EthicsPoint Hotline.

Our Pledge to One Another

Diversity and Inclusiveness

As a global organization, our employees, clients and partners are naturally diverse. We treasure diversity because it brings a broader range of perspectives and capabilities to our organization. This provides an advantage for our shareholders, clients, communities and other stakeholders. One of our business objectives is to provide the best match of talent to our clients to help everyone achieve more than they imagined. Diversity is essential to maintaining our role as an expert in IT delivery services and to our ability to meet the needs of our clients by being open to the ideas of all and allowing everyone to reach their potential.

Individual Privacy

Our respect for people means that we respect and protect the sensitive personal information about our employees, associates, clients, vendors, candidates and partners and individuals. Personal data such as identification numbers, home addresses, telephone numbers, personal medical information and other data must be kept confidential and is to be used only for legitimate business purposes.

Many countries in which we operate have specific laws about data privacy. We recognize the need to protect personal privacy and are committed to handling personal data in a responsible manner and in compliance with those laws.

We understand data privacy requirements and use personal data contained on Ciber systems, intranet, email and other applications only for legitimate business purposes. Our company respects people's work spaces, including email and voicemail. The company also has certain legal rights to encourage our ethical behavior. This includes full access and inspection of things like computer files, telephone records, email, voicemail, Internet use, business documents, desks, lockers and other company property. When we show respect for each other and all stakeholders, we also show respect for the use of company services, facilities and equipment.

Ciber wants to protect people's rights and information and be compliant with government regulations regarding protection of data privacy laws that impact our business.

Harassment and Non-Discrimination

Ciber prohibits sexual harassment as well as any harassment because of race, color, gender, religion, age, national origin or ancestry, disability, veteran status, marital status, as well as any other category protected by federal, state, or local laws. We will also not tolerate verbal, nonverbal or physical conduct by anyone associated with our business (including clients or subcontractors) that harasses or creates an intimidating, offensive, abusive or hostile work environment, including any workplace violence or harassment. All such harassment is unlawful and will not be tolerated. We are committed to providing equal opportunities in employment. This means we must treat our fellow employees and applicants fairly and with respect and never engage in any form of unlawful discrimination. We follow all related laws and in our employment decisions (such as recruiting, hiring, training, salary determination and promotion) we do not discriminate against individuals on the basis of race, color, gender, age, national origin, religion, sexual orientation, gender identity and expression, marital status, citizenship, disability, veteran status, HIV/AIDS status, or any other legally protected factor.

Real World Scenario
Unwelcome conduct may be conduct that is unwanted, uninvited or uninitiated. Conduct that may be acceptable for one person may be unwelcome for another (such as a joke or a hug). The determination about potential harassment does not depend on the intent of the alleged harasser; instead, it depends on the person receiving or witnessing the conduct and considering it to be unwelcome.

For example, "Joe" often greets female employees with a hug. Joe is friendly to male co-workers too, but generally just gives them a slap on the back. What Joe doesn't realize is that although most co-workers don't mind this behavior, one co-worker cringes every time she hears Joe coming because she is very uncomfortable when he hugs her. Joe needs to understand that even though he has good intentions, his conduct could be the basis for a sexual harassment complaint because it is unwelcome to at least one co-worker.

We all have a personal responsibility for maintaining a safe and respectful work atmosphere, free of abusive or unprofessional conduct. Every employee is expected to respect their colleagues as individuals and to treat them with dignity.

Harassment Defined

Sexual harassment is defined by applicable state and federal laws as unwanted sexual advances, requests for sexual favors or visual, verbal or physical conduct of a sexual nature when: (1) submission to the conduct is made as a term or condition of employment, or (2) submission to or rejection of the conduct is used as a basis for hiring decisions affecting the individual, or (3) the conduct has the purpose or effect of unreasonably interfering with the employee's work performance or creating an intimidating, hostile or offensive work environment. This definition includes many forms of offensive behavior.

The following is a partial list of harassing behaviors:

- Unwanted sexual advances or propositions of any nature.
- Offering employment benefits in exchange for sexual favors.
- Making or threatening reprisals after a negative response to sexual advances.
- Visual conduct such as leering, making sexual gestures or displaying sexually suggestive objects, pictures, cartoons or posters.
- Verbal conduct such as making or using derogatory comments, epithets, slurs, sexually explicit jokes or degrading comments.
- Verbal abuse of a sexual nature or suggestive or obscene letters, notes or invitations.

Sexual harassment occurs whenever unwelcome conduct of a sexual nature affects a person's job. Such conduct includes unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature and is not tolerated by Ciber.

Harassment on the basis of race, color, sex, religion, age, national origin or ancestry, disability, veteran status, marital status, as well as any other category protected by federal, state, or local laws includes behavior similar to sexual harassment:

- Verbal conduct such as threats, epithets, derogatory comments or slurs.

- Visual conduct such as derogatory posters, photographs, cartoons, drawings or gestures.
- Physical conduct such as assault, unwanted touching or blocking normal movement.
- Retaliation for reporting harassment or threatening to report harassment.
- Verbal conduct such as threats, epithets, derogatory comments or slurs.

Prohibition of Harassment

An employee of Ciber, whether a coworker or manager, who is found to have engaged in harassment is subject to disciplinary action, up to and including termination of employment. Any manager or supervisor who knew about harassment and took no action to stop it or failed to report the harassment to management may also be subject to discipline, up to and including termination. We do not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, we reserve the right not to provide a defense or pay damages assessed against employees for conduct in violation of this policy.

Reporting of Harassment

As our complaint procedure provides for an immediate, thorough, and objective investigation of any claim in violation of this policy and appropriate disciplinary action, we encourage anyone who feels harassment has taken place to contact your Human Resources manager, Vice President of Human Resources or use one of the resources identified in the Complaint Procedure section within this Code to report the action verbally or in writing.

Workplace Safety

The health and safety of employees and others on Ciber property or assigned to client sites are of critical concern to us. We strive to attain the highest possible level of safety in all activities and operations. We care about the health and safety of everyone as an integral part of our culture. With these values in mind, Ciber intends to comply with all health and safety laws applicable to our business.

To this end, we must rely upon you to ensure that work areas are kept safe and free of hazardous conditions. Safety is every employee's responsibility; each of us is expected to exercise maximum care and good judgment at all times to prevent accidents and injuries. Everyone must fully comply with all safety and health regulations, policies and procedures. Inform your supervisor immediately about any potential hazards, unsafe conditions, equipment or practices, and do everything reasonable to keep Ciber a safe place to work. We must all report unsafe working conditions or practices immediately so that timely action may be taken. If you are working at client sites, you are expected to familiarize yourself with and follow all safety- related policies associated with working on that client site. Work-related injuries, no matter how minor, should be reported without delay in accordance with the Worker's Compensation policy described in the Employee Benefits section of the Employee Handbook and on Ciber's internal website.

Workplace Violence

Workplace violence can include robbery and other commercial crimes, domestic and stalking cases, violence directed at the employer, past or current employees and family members, clients, Ciber partners, and other third parties. Subject to applicable laws and regulations, we prohibit the possession and use of firearms, other weapons, explosive devices and other dangerous materials on company property, client sites, or while conducting company business.

Substance Abuse

Ciber is committed to providing a drug-free and alcohol-free workplace. Everyone must be free of the physical and psychological influences of drugs and alcohol while conducting company business and while on company property to maintain a safe and pleasant working environment. Reporting to work under the influence of alcohol or drugs, or using, possessing or selling illegal drugs while on company time or property or client sites may result in immediate termination.
The purchase or consumption of alcoholic beverages on company property is prohibited except when specifically authorized by company management at company functions. If you are using prescription drugs that may have an effect on your work performance or compromise your ability to work safely, discuss this with your manager or supervisor.

Our Accountability to Our Shareholders

Conflicts of Interest

We want to avoid issues that may arise when your personal interests (business, financial, civic or professional) conflict with the interests of the company and/or with their loyalty, judgment or decision-making. Even the appearance of a conflict of interest can be harmful, because it may look like poor judgment was used.

These rules also apply to your immediate family members and other relatives or individuals living in your home. Immediate family members include spouse or same-sex domestic partner, child, parent, sibling, grandparent, grandchild, in-law (mother, father, sibling) and step-relatives (father, mother, sibling, child).

Likely areas of conflicts of interest include:

- Do not use company time, materials, equipment, information or other assets (for example, trade secrets, client or vendor information, etc.) for personal purposes and/or financial gain.
- Do not participate in a decision to select a vendor, contractor or subcontractor with which employee has a personal interest.
- Do not take advantage of business opportunities reasonably available to Ciber.

Contact the Legal Department to report a possible conflict of interest or if further assistance is needed. Disclosure is crucial for resolution.

To assist you in determining if you have a conflict of interest in a particular situation, you should consider the following:

1. Whether you or any member of your immediate family or household have been a director, officer, owner, partner, employee, agent, consulting company, contractor or subcontractor of a firm that is a competitor, client or supplier of Ciber's or whether you are in a close business or personal relationship with anyone associated with that firm;

2. Whether you have proprietary information from a prior employer;

3. Whether you or any member of your immediate family or household has more than a one percent financial interest in any firm that is a competitor, client or supplier of Ciber's and, if so, are you or any of your direct reports involved with decisions, contracts, recommendations, etc. with respect to such firms;

4. Whether you or any member of your immediate family or household is in an elected or appointed office or advisory position in federal, state or local government; and

5. Whether there is any other business or personal situation that you feel could be interpreted as an actual or potential conflict of interest.

Compliance with Trading in Securities

Because the common stock of Ciber, Inc. is traded publicly on the New York Stock Exchange (NYSE) under the symbol "CBR", securities laws place certain restrictions on Ciber employees in the buying and selling of Ciber stock or publicly traded options to buy or sell Ciber stock.

Specifically, U.S. Federal securities laws prohibit buying or selling company stock at a time when you are aware of material information about Ciber that is not publicly known. Trading in this situation is called "insider trading." This law also prohibits you from passing on such information to others who might then trade in company stock.

As Ciber employees have material (see next section regarding Material Information), non-public information relating to Ciber or any of its subsidiaries, Ciber employees may not buy or sell Ciber securities or engage in any other action to take advantage of, or pass on to others, that information. Transactions that may be necessary or justifiable for independent reasons, such as the need to raise money for an emergency expenditure, are no exception.

In addition, if you have material, non-public information relating to any proposed acquisition of, or business combination with, any public company or any other financial or other material information regarding any other public company arising out of your position with the Company, you may not buy or sell securities of that company or engage in any other action to take advantage of, or pass on to others, that information.

Material Information

Material information is any information that a reasonable investor would consider important in a decision to buy, hold or sell stock (i.e., any information that could affect the price of the stock). Examples of material information include news of current earnings or losses, projections of future earnings or losses, news of a pending or proposed merger, acquisition or tender offer, changes in dividend policies, the declaration of a stock split, the offering of additional securities, changes in management, and financial liquidity matters. Either positive or negative information may be considered material. If you have material information about Ciber, you must not pass the information on to others who may use the information to buy or sell Ciber stock for their own accounts. Anyone with access to such information must keep it confidential and not discuss it with anyone outside of Ciber including business contacts, family members or friends.

Transactions by Family Members

The same restrictions apply to your family members and others living in the household. You are responsible for the compliance by your immediate family and personal household members.

Accurate Books and Records/ Public Disclosure of Company Information

It is extremely important that financial and other disclosure provided in Ciber's reports and documents

filed with or submitted to the United States Securities and Exchange Commission ("SEC") and in other public communications made by Ciber be full, fair, accurate, timely and understandable. While our Chief Executive Officer, Chief Administrative Officer, Chief Financial Officer, Controller and other company employees performing similar functions are primarily responsible for compliance with these disclosure requirements, all company employees are accountable within the scope of their duties for ensuring that our accounting, financial and other systems provide accurate and timely reporting of transactions involving Ciber assets so that, among other things, the SEC reports and other public communications about Ciber represent the company's financial and non-financial information in a full, fair, accurate, timely and understandable manner. Every accounting or financial record, as well as the underlying support data, must accurately describe transactions without omission, concealment, or falsification of information, and must comply with applicable accounting standards.

"Books" are defined as documents (including electronic files) containing accounting, inventory, financial, securities and corporate information.

"Records" are defined as all information recorded for the Company, such as:

- Employee time reports and payroll records (i.e. overtime, Personal Time Off or other exception time).
- Sales transactions and billing records.
- Purchasing transactions, including bills and invoices.
- Permits and licenses.
- Government reports.
- Expense account records.

Questions about requirements for financial reporting may be directed to the Chief Financial Officer. In addition, anyone can submit a complaint regarding accounting, internal controls, auditing, or other matters through the Ciber's anonymous and confidential EthicsPoint hotline is located at: www.ciber.ethicspoint.com

Document Management and Retention

You are responsible for protecting, maintaining and destroying records appropriately. Records include information in paper documents and electronic files found on computer hard drives, file servers, e-mail, disks, CDs, microfilm, DVDs, databases (including PMRx or Ciber records on customer databases) or any other media. You must manage records in a consistent manner to provide an accurate audit trail of the Ciber's business transactions.

The length of time a record must be kept is determined by business and legal requirements. When records are no longer needed, they must be destroyed according to the retention schedule outlined in the Company's Document Retention Schedule accessible on Ciber's internal website unless such records are subject to legal hold issued by the Ciber's Legal Department. Such records can only be destroyed according to the retention schedule when the Legal Department has released the legal hold. Timely destruction reduces the cost of space, equipment and personnel necessary to store, organize and handle the high volume of records. It also helps Ciber meet legal requirements established by federal, state and/or local laws, regulations and statutes.

You should review your records on an annual basis, if not more often. See our Document Retention Schedule on Ciber's internal website for more information.

Communications with the Financial Community and Media

We have designated certain spokespersons as the only employees who can discuss certain information with the news media and financial community.

Communications with the Financial Community

You must not discuss with anyone in the financial community (i.e., stockbrokers, analysts, etc.) business conditions of Ciber. If you receive a call from a stockbroker or analyst, you must not offer any comment about the business condition or clients of Ciber. Instead, you should respond by saying that it is our company's policy for these matters to be handled by the Director of Finance who may be contacted at Ciber's corporate office.

Communications with the Media

If you receive a call from an editor or reporter representing local newspapers, TV/radio stations or other business/

financial publications, you should refer the caller to the Director of Finance or Director of Corporate Communications at the corporate office. These individuals can then arrange for interviews with the appropriate person. However, appropriate management personnel may handle routine calls from the trade press that do not involve discussions of business or finance.

Use of Social and Electronic Media

Ciber encourages the responsible use of social networks for business-related and professional networking purposes. Any employee of Ciber, by virtue of identifying themselves as such within a social network, is creating perceptions about themselves by their colleagues and managers; in addition they are creating perceptions about their expertise and about Ciber by our shareholders, customers and general public. It is important that you are aware of the implications of engaging in forms of social media and online conversations that reference Ciber, your relationship with Ciber, and Ciber products and services. It is also important to recognize that Ciber may be held responsible for your content posted on social network sites. You are required to comply with Ciber's Social Media Policy accessible on Ciber's internal website and social media should never be used in a way that violates any other Ciber policy or employee obligation. You should not initiate or respond to comments related to the trading of Ciber stock, company operating results, non-public information (i.e., new client contracts or any other client-specific information), or any form of communication that could be construed as insider information about the company, whether negative or positive.

Online social networks are a big part of our success, connecting us with fans and friends who have become clients and colleagues. We encourage and empower employees to use social networks appropriately. We expect employees' online behavior to mirror their behavior in any company setting. Please refer to the Social Media Policy for guidelines.

Our brand and reputation depend on each of us and how we conduct ourselves. This includes conduct via all electronic media and communications systems such as voicemail, email and commercial software.

Communications on these systems are not private. Communications via voicemail, email and other commercial software are considered business records. Therefore, Ciber may, in accordance with applicable legal regulations, limit, read, access, intercept and disclose the contents of these communications.

As users of these systems, we are responsible for ensuring that communications on these systems do not harm or offend anyone, or expose our company to risk. We must never use Ciber's systems to knowingly, recklessly or maliciously post, store, transmit, download or distribute any threatening, abusive, libelous, defamatory or obscene materials of any kind.

Real World Scenario
Steve, a client partner, shows his co-worker, Joe, a comment he is about to post on a social networking site regarding the latest news on the world's debt. Joe expresses concern that Steve is posting under his Ciber email, and points out that it could appear that the opinion being expressed is Ciber's rather than Steve's. Steve responds that there is nothing in the Code of Conduct that forbids this, but Joe stresses that the Code cannot specifically address every situation and that Steve could be in trouble if someone mistakes his opinion for Ciber's position.

Joe has a valid point. By understanding and applying the intent of the Code, we are all expected to make good decisions about what is appropriate use of company resources. The Code clearly states that Ciber assets such as email addresses are to be used for business purposes, and we have a responsibility to act in the company's best interests. If Steve's opinion were reported in the news media as Ciber's, it could reflect badly on the organization.

Always use common sense guided by the intent of the Code, and if you need help, ask your supervisor.

Other Requests for Information

Any releases of information relating to Ciber (except normal material given to suppliers or clients) should be coordinated with Ciber management and the Legal Department as appropriate. Releases of information relating to employees, suppliers, or clients must be coordinated with the Legal Department to ensure compliance with applicable laws protecting the privacy and property rights of those parties.

Our Obligation to Protect Assets and Information

Confidentiality

We expect all employees to respect the confidential information of Ciber, Ciber subcontractors and Ciber clients (collectively “Ciber and client information”) with which they may be entrusted. Ciber and client information includes any information that derives value from not being generally known to other persons, including, but not limited to, methods and techniques, client lists and profiles, business operations, data, finances, accounting procedures, billing rates, contractor fees, marketing and sales strategies, projections, estimates, tax records, employee lists, candidate lists, employee compensation, personnel history, existing and future products and services of Ciber and its clients. Ciber considers all such information to be trade secrets and intellectual property of Ciber, and expects company employees to do the same.

You may use Ciber and client information in the general course of doing business; however, all Ciber and client information must be safeguarded against loss, damage, misuse, theft, fraud, sale, disclosure or improper disposal.

Ciber and client information may not be used for personal purposes or disclosed outside the company. Doing so could damage Ciber competitively or financially. In addition, the confidential information of others may not be copied without the owner's written permission. For example, do not reproduce, distribute or alter material from books, trade journals, magazines or licensed computer software, or use music or videotapes without the owner's written authorization.

If you leave Ciber, you remain legally obligated to not disclose Ciber and client information to any new employer or anyone else who has not signed an appropriate non-disclosure agreement with Ciber or Ciber's clients. Ciber and client information also includes information regarding the particular skill sets, assignments or expertise of Ciber's employees. Accordingly, you may not share this information with your new employer to facilitate the new employer's recruitment of Ciber personnel.

Any disclosure of this information may subject you to legal liability in an action brought by either Ciber or the client against you.

Real World Scenario
Monica, a Ciber consultant, tells her best friend John about a new tool Ciber has developed that will help increase our revenue. Monica tells John not to share this information with anybody, especially his cousin who is an executive at a rival company. John promises to be discrete, despite proving unable to keep secrets in the past. Monica could be exposing an important company secret. Common sense should tell her that sharing this information outside the company, especially with a relative of a competitor is extremely unwise. She should not divulge confidential information about the company or its business under any circumstances. All Ciber employees are expected to respect Ciber's assets as they would their own.

Protection and Use of Company and Client Assets

It is everyone's responsibility to know these guidelines, and to conduct their activities accordingly.

You are responsible for the appropriate use, maintenance and protection of Ciber and client assets from theft, damage or loss whether on or off company or client premises.

The term "assets" includes but is not limited to:

- Any data, intellectual property (IP) of Ciber or our clients, computer hardware and software, network services such as telephone, voice mail, facsimile, email, Internet access and third-party services.
- Cell phones and mobile devices.
- Copiers, supplies and records.
- Company funds and financial assets.

These assets are to be used for business purposes in serving the interest of the company and of our clients in the course of normal operations. You should be aware that the data and documents you create on the corporate assets remains the property of Ciber.

For security, network maintenance and other purposes, authorized individuals within Ciber may monitor equipment, systems and network traffic at any time.

Here are some ways you can protect Ciber and client funds and property:

- Make sure expenditures are only for authorized and legitimate business purposes.
- Keep accurate and complete records of funds spent.
- Use corporate charge cards only for business purposes.
- Make sure Ciber and client assets (including passwords and other methods used to access or transmit data) and the information they contain are protected against unauthorized access, use, modification, destruction, theft, loss or disclosure.
- Use telephones, e-mail and the Internet only for legitimate business purposes. While some incidental personal use may be permitted, these means of communication must never be excessive or used for illegal purposes, or in a manner inconsistent with Ciber's policies and this Code.

- Plan travel well in advance and book appropriately to get best travel rates.

Company Funds

Company funds may not be used for personal purposes. If you are issued a corporate credit card, it may only be used for business purposes. Ciber may recover unauthorized expenses from you that are inappropriately classified as business. If you submit unauthorized expenses, corrective action could be taken against you up to and including termination.

Actual or suspected loss, damage, misuse, theft, embezzlement, or destruction of company funds or company or client property must be reported immediately to the Chief Financial Officer or General Counsel.

Intellectual Property

We are also obligated to safeguard any intellectual property (IP) of Ciber or our clients, even if public, which includes our trademarks, patents, copyrights and inventions. Please note that Ciber owns the copyright in works and the patent rights in innovations that you develop during the course of your employment. Your obligation to protect this information continues even after your employment ends. At that time, you must return all confidential and proprietary information in your possession.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Ciber.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or video, and the installation of any copyrighted software for which Ciber or the end user does not have an active license is strictly prohibited.

- Introduction of malicious programs into the network (e.g., viruses, works, Trojan horses, e-mail bombs, etc.).

- Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is part of your normal authorized job function.

- Circumventing user authentication or security of any host, network or account.

Under no circumstances are you, as an employee of Ciber, authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Ciber or client-owned resources.

Our Responsibility to Our Customers and Business Partners

Client Relationship

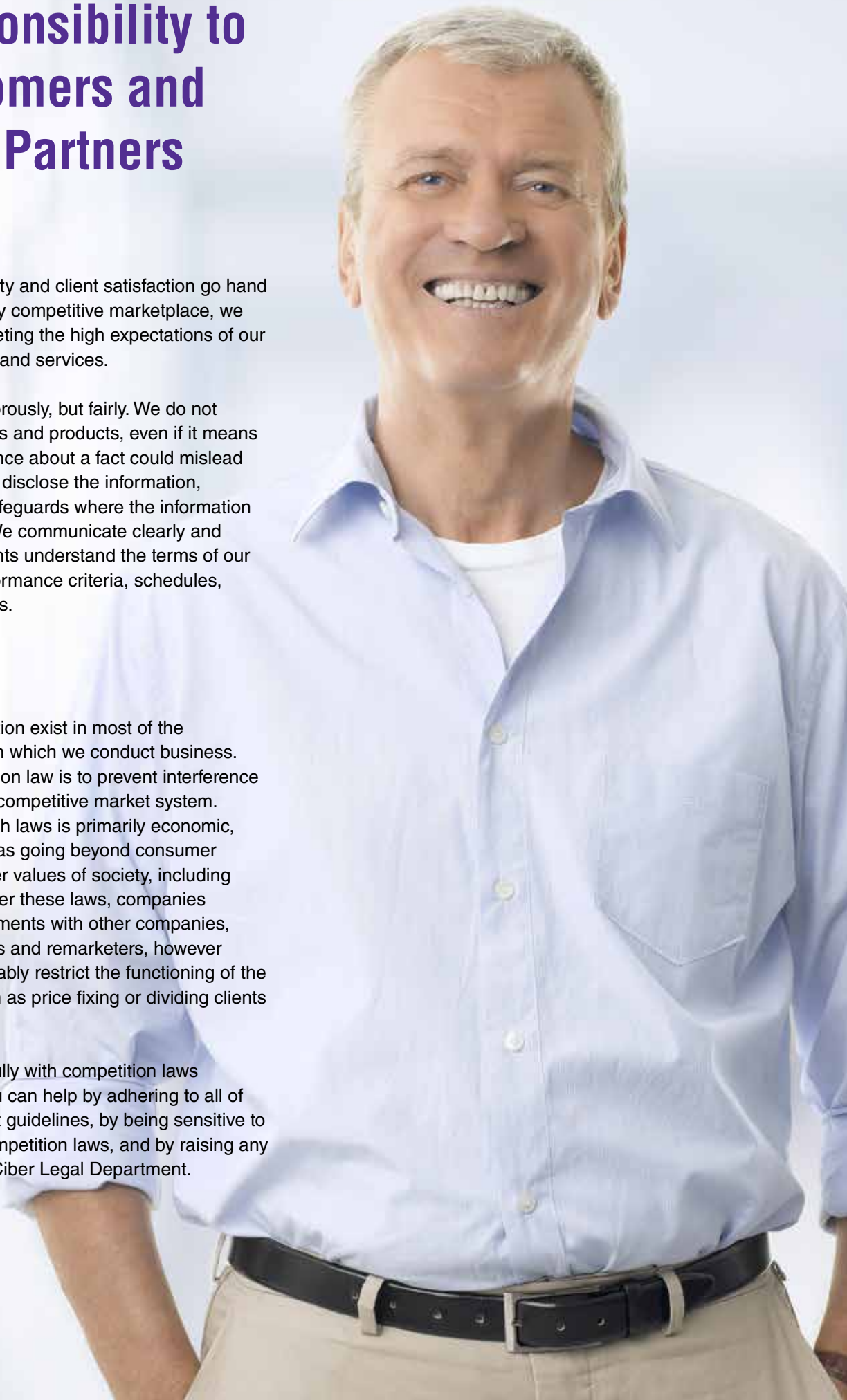
We recognize that integrity and client satisfaction go hand in hand. In today's fiercely competitive marketplace, we can succeed only by meeting the high expectations of our clients with our products and services.

You should compete vigorously, but fairly. We do not misrepresent our services and products, even if it means losing a sale. Where silence about a fact could mislead a client, employees shall disclose the information, subject to appropriate safeguards where the information is confidential to Ciber. We communicate clearly and precisely so that our clients understand the terms of our contracts, including performance criteria, schedules, prices and responsibilities.

Competition

Laws governing competition exist in most of the industrialized countries in which we conduct business. The purpose of competition law is to prevent interference with the functioning of a competitive market system. While the purpose of such laws is primarily economic, their effect is often seen as going beyond consumer welfare to protecting other values of society, including individual freedoms. Under these laws, companies may not enter into agreements with other companies, including their distributors and remarketers, however informally, that unreasonably restrict the functioning of the competitive system, such as price fixing or dividing clients or territories.

Our policy is to comply fully with competition laws throughout the world. You can help by adhering to all of Ciber's business conduct guidelines, by being sensitive to legal concerns under competition laws, and by raising any such concerns with the Ciber Legal Department.



Real World Scenario
You are at a trade association meeting when you are invited to meet informally with representatives from several competitors. At the meeting, one of them mentions a new tax that will make it more expensive to do business in a particular region. Another person suggests that everyone should agree to a slight price increase to a particular product line to offset the new tax.

In this situation, collaborating with competitors to set prices is a violation of U.S. antitrust laws and global competition laws. Even being in the room during a discussion like that can result in severe penalties. In this situation, decline to discuss the issue and remove yourself from the situation. It is not enough to stay quiet; you must actively protest. You should certainly not take notes, nor should you suggest that Ciber use such illegal practices. You should also advise Ciber's Legal Department of the incident.

Remember that violation of antitrust and competition laws do not require a formal, written agreement. If the competitors at that meeting said nothing further about the tax and price increase, but some of the attendees subsequently did raise their prices to offset the new tax, those facts may be enough for a prosecutor to commence an investigation.

Gathering Competitive Information

Gathering information about competitors, when done legally and ethically, is a legitimate business activity. It enhances our knowledge of the marketplaces in which we sell and helps us understand and meet client needs.

However, competitive information should never be obtained – directly or indirectly – by improper means such as misappropriation of proprietary information, bribing a competitor's employee, or misrepresenting the fact that one is a Ciber employee including obfuscation, or hiring a consulting company to engage in any of this conduct. There are also other ways competitive information could come to your attention, such as at trade shows, trade association gatherings, or other types of meetings with competitors. In such cases, you may not participate in discussions with competitors about pricing, profit margins or costs, bids, terms or conditions of sale, sales territories, market share, distribution practices, or other competitive information. Not only do these types of conversations pose the risk of you obtaining proprietary information through inappropriate means, they also can create the appearance or form the basis of a price fixing conspiracy among competitors. Such activities generally are illegal under antitrust and competition laws. If you find yourself involved in this type of discussion, excuse yourself and immediately report the incident to the Legal Department.

Relationships with Suppliers

We strive to build good working relationships with our suppliers including, specifically, our independent contractors and subcontractors. They are instrumental in helping us achieve the highest standards of quality in satisfying our clients. We consider multiple factors when selecting suppliers. These factors include, among other things, price, quality, delivery capacity, reputation for service and integrity, and the supplier's status as a client of Ciber services.

We have negotiated certain contracts with vendors for discounts on high-volume purchases – such as travel, office supplies, and cellular and long distance services in order to help lower operating expenses. You must justify to your supervisor the selection of alternative vendors before purchasing products and services from them.

Gifts and Entertainment

You may not request or accept gifts or entertainment that may influence judgment in favor of a particular supplier or client over others. A supplier is any company or person (such as a consulting company, contractor or subcontractor) who sells services or products to Ciber and is not an employee.

You and your immediate family members and other individuals living in your home may accept gifts or entertainment or have a meal or drinks or attend an event that includes lodging and transportation with a vendor or client, or accept a free or discounted product, service, gift or other favor from a vendor or client only if the gift or entertainment is:

- unsolicited;
- provided to others in the normal course of doing business;
- for a legitimate business purpose;

- such that it does not cause an employee to favor a particular supplier or client over others;
- not improper, offensive or otherwise in conflict with corporate policies; and
- not in violation of a law.

You may provide gifts and reasonable entertainment to a supplier or client as long as you meet the above conditions and do not influence a business decision.

Promptly return unacceptable gifts to the supplier. If returning the gift is impractical (such as perishable fruit, etc.), donate it to charity in the supplier's name. Send the supplier a thank you letter but explain the disposition of the gift and Ciber's policy regarding gifts.

Certain laws strictly prohibit offering or giving anything of value to a government employee involved in a pending procurement. Ciber policy and laws strictly forbids the offering or giving of anything of value to government employees who work in government agencies that may be involved in decisions to purchase services or products from Ciber. This Ciber policy applies to state, local and foreign government employees involved in procurement decisions as well as federal government employees.

Real World Scenario
"Julia" is given tickets to the World Cup championship soccer game as a thank you for using a particular vendor's services. Before Julia accepts the tickets, she checks if a conflict exists by asking herself "Is it legal?", "Is it consistent with Ciber values, the Code of Conduct, and Ciber policies?" and "Would others think it was ok if they read it in a news story?"

If Julia accepts free tickets from a vendor, she is creating an apparent conflict of interest and jeopardizing Ciber's reputation. Julia may also feel obligated to use the vendor for future business even if the vendor does not produce satisfactory work. Because she is not 100% sure what to do next Julia contacts the General Counsel for advice.

Our Duty as Responsible Global Corporate Citizens

Compliance with Laws

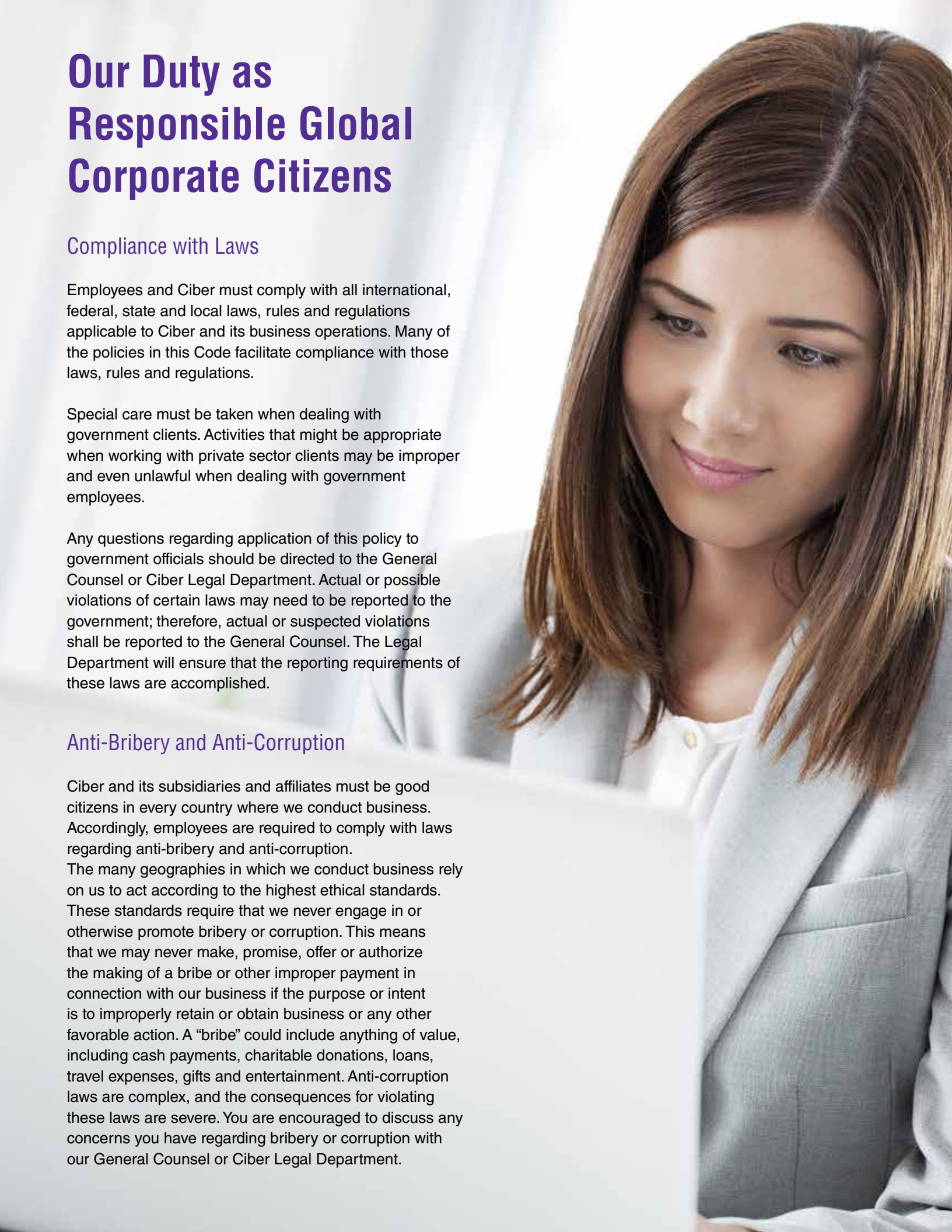
Employees and Ciber must comply with all international, federal, state and local laws, rules and regulations applicable to Ciber and its business operations. Many of the policies in this Code facilitate compliance with those laws, rules and regulations.

Special care must be taken when dealing with government clients. Activities that might be appropriate when working with private sector clients may be improper and even unlawful when dealing with government employees.

Any questions regarding application of this policy to government officials should be directed to the General Counsel or Ciber Legal Department. Actual or possible violations of certain laws may need to be reported to the government; therefore, actual or suspected violations shall be reported to the General Counsel. The Legal Department will ensure that the reporting requirements of these laws are accomplished.

Anti-Bribery and Anti-Corruption

Ciber and its subsidiaries and affiliates must be good citizens in every country where we conduct business. Accordingly, employees are required to comply with laws regarding anti-bribery and anti-corruption.
The many geographies in which we conduct business rely on us to act according to the highest ethical standards. These standards require that we never engage in or otherwise promote bribery or corruption. This means that we may never make, promise, offer or authorize the making of a bribe or other improper payment in connection with our business if the purpose or intent is to improperly retain or obtain business or any other favorable action. A “bribe” could include anything of value, including cash payments, charitable donations, loans, travel expenses, gifts and entertainment. Anti-corruption laws are complex, and the consequences for violating these laws are severe. You are encouraged to discuss any concerns you have regarding bribery or corruption with our General Counsel or Ciber Legal Department.



Anti-boycott

All Ciber employees are prohibited from complying with or supporting a foreign country's boycott of a country unless a qualifying exception is allowed. Due to our global operations, we must be alert for illegal boycott requests. A "boycott" is a term used to describe situations where one person, group or country refuses to do business with certain persons, groups or countries as a means of protest. Ciber is also required to report promptly to the U.S. Government any request to support a boycott or to furnish information concerning a boycott. You should advise the Legal Department of any such request.

Political Contributions and Activities/Lobbying

Ciber complies fully with all federal, state, local and foreign laws governing the contribution of funds or assets to candidates for political office or to political parties. As a general rule, Ciber does not contribute corporate funds or make in-kind corporate contributions to candidates for political office and no employee or agent may make or approve such contributions on behalf of Ciber.

Any request for or interest in Ciber making a contribution to a political candidate or party must be forwarded to and handled by Ciber's General Counsel. Any questions regarding this policy should be directed to the Legal Department.

Because lobbying and lobbyists are regulated by the law, you may not engage in lobbying on behalf of Ciber or engage others to do so unless specifically requested to do so by a Ciber officer in consultation with the Legal Department.

Any suspected violations should be reported to the Chief Financial Officer or the General Counsel.

Environmental Stewardship

Ciber's commitment to the communities we serve means we are constantly striving to reduce our environmental impact. We operate our facilities with the necessary permits, approvals and controls. We continue to learn more and better ways to go beyond compliance with the environmental laws and standards that apply to us.

We can play a key role and have a positive impact on the environment by modeling good choices and using opportunities to encourage responsible stewardship of the environment by our employees, clients, Ciber partners and others. In this way, Ciber can help support more sustainable communities in which to live and work. Based on the principal of "Reduce, Reuse and Recycle," most of Ciber's environmental initiatives are implemented at the local level with programs that respond to local and national needs. We encourage employee ideas and participation in environmental programs in each business unit.

Our Ciber India office, in a LEED Gold Certified building, is a model that demonstrates how location, construction materials, energy and water conservation and operating principles can reduce environmental impact and create a pleasant experience. Our intention is to use this model for all of our locations, to the extent that is practical. Operational functions should always consider ways to improve environmental outcomes, and, as a result, encourage individuals to apply similar principles in their personal lives.

Questions and Resources

As a reminder there are a number of resources available to you. It is important to contact one of the following when there is a question or concern:

- Your manager.
- Any other Ciber manager.
- A functional or geographic leader.
- Any member of the Executive Leadership Team (ELT).
- The Compliance Committee.
- One of the following at the Ciber Corporate office by dialing 800-242-3799.

  - Ciber's Vice President of Human Resources.

  - Ciber's General Counsel.

Please note this Code of Conduct does not constitute an employment contract and does not offer employment for any length of time.

ciber®

Ciber | 6363 South Fiddler's Green Circle, Suite 1400, Greenwood Village, Colorado 80111, USA
Tel. (800) 242.3799 | info@ciber.com | www.ciber.com