

# ***CIBER's Code of Business Conduct and Ethics***

## **Introduction**

CIBER believes that good ethics are the basis for good business practices that will produce the best results for our shareholders. CIBER's Code of Business Conduct and Ethics contains the ethical principals 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 (hereinafter "CIBER" or the "Company"), all of whom will be referred to as "employees" or "you" and "yours" in the Code. This Code supplements the other policies and procedures found on CIBERspace.

Since CIBER's independent contractors and subcontractors represent CIBER in their business dealings, they must also comply with our policies. CIBER employees are responsible for educating the independent contractors and subcontractors about the policies to ensure they meet the requirements of CIBER's Code of Business Conduct and Ethics.

The Company will review and revise these 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. **This Code of Conduct does not constitute an employee contract and does not offer employment for any length of time.**

## **Conflicts of Interest**

The Company wants to avoid issues that may arise when employee's 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 employees' immediate family members and other relatives or individuals living in their 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 are listed below.

- 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.

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

1. Whether employee or any member of their 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 they are in a close business or personal relationship with anyone associated with that firm;
2. Whether employee has proprietary information from a prior employer;

3. Whether employee or any member of their 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, is employee or any of their direct reports involved with decisions, contracts, recommendations, etc. with respect to such firms;
4. Whether employee or any member of their 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 employees feel could be interpreted as an actual or potential conflict of interest.

Contact the Law Department to report a possible conflict of interest or if further assistance is needed.

### **Confidentiality**

CIBER expects all its employees to respect the confidential information of CIBER, CIBER subcontractors and CIBER clients (collectively "CIBER Information") with which they may be entrusted. CIBER Information includes any information that derives economic 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, 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 expects its employees to do the same.

Employees may use CIBER Information in the general course of doing business; however, all CIBER Information must be safeguarded against loss, damage, misuse, theft, fraud, sale, disclosure or improper disposal.

CIBER Information may not be used for personal purposes or disclosed outside the Company. Doing so could hurt the Company, 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.

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

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

### **Protection and Use of Company and Client Assets**

Whether on or off Company property, employees are responsible for the appropriate use, maintenance and protection of Company and client physical property from theft, damage or loss. Physical property includes but is not limited to:

- Computer hardware and software, network services such as telephone, voice mail, facsimile, e-mail and Internet access
- Cell phones and pagers
- Copiers, supplies and records
- Company funds and financial assets

Here are some ways to protect Company (and client, where appropriate) funds and property:

- Make sure expenditures are for legitimate business purposes.
- Keep accurate and complete records of funds spent.
- Use corporate charge cards only for business purposes.
- Make sure Company and client computer and communications equipment and systems (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 CIBER's trademarks and service marks in accordance with Company instructions.
- 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.

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

Actual or suspected loss, damage, misuse, theft, embezzlement, or destruction of Company funds or Company or client property should be reported immediately to the Chief Financial Officer.

### **Compliance with Laws/Trading in Securities**

Employees and CIBER must comply with all 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.

In particular, because the common stock of CIBER, Inc. is traded publicly on the New York Stock Exchange (NYSE) under the symbol "CBR", the 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. Accordingly, if a director, officer, or any employee has material, non-public information relating to CIBER or any of its subsidiaries, neither that person nor any related person may buy or sell securities of the Company 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, no director, officer, or any employee who has 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 his or her position with the Company, may 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. Employees who have material information about CIBER must not pass the information on to others who may use the information to buy or sell CIBER stock for their own accounts.

### Transactions by Family Members

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

### **Open Door Policy/ Ethics Compliance**

Every employee has a responsibility to maintain and advance the business ethics reputation of the Company and its employees. It is 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. All employees 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.

CIBER believes that open communication is essential to a successful, ethical work environment and all employees should feel free to raise issues of concern without fear of reprisal. CIBER employees have an "open door" to any level of management including the President of the Company. Differing opinions and expressions of concern are welcome. While we may 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, CIBER employees can take that concern or complaint to a supervisor. If the complaint is about the supervisor, or if the supervisor cannot solve the problem, CIBER employees may take the matter to higher management or other appropriate persons without fear of reprisal or retaliation. Although CIBER cannot guarantee that every concern or complaint will be resolved to employee's 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, the Company will keep complaints and their resolution confidential. Employees are expected to cooperate in Company investigations and answer questions truthfully to the best of their ability. Employees should not undertake investigations on their own. If an employee believes a potential violation of a policy or the law occurred, please contact either the General Counsel in the Law Department or the Director of Human Resources.

Where an audit or investigation reveals the need to take corrective measures, employees have an obligation to cooperate in 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 an ethical infraction 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. At sites performing work under certain government contracts, ethics violations may also result in a withdrawal or denial of an individual's security access by the issuing authority, which may or may not impact continued employment.

## **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 the Company's Chief Executive Officer, Chief Financial Officer, Chief Accounting 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 CIBER's accounting, financial and other systems provide accurate and timely reporting of transactions involving Company assets so that, among other things, the SEC reports and other public communications about the Company 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 Accounting Officer or Chief Financial Officer. In addition, CIBER's Audit Committee has established a complaint procedure for the receipt, retention, and treatment of complaints received by CIBER regarding accounting, internal controls or auditing matters. This procedure allows for the confidential, anonymous submission by employees of CIBER of concerns regarding questionable accounting or auditing matters and can be found on the Company's website at [www.ciber.com](http://www.ciber.com), under Investors, Corporate Governance.

### ***Records Management***

Employees 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, microfiche, or any other media. Employees must manage records in a consistent manner to provide an accurate audit trail of the Company'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 Records Management Operations Plan. Timely destruction reduces the cost of space, equipment and personnel necessary to store, organize and handle the high volume of records. It also helps the Company meet legal requirements established by federal, state and/or local laws, regulations and statutes.

Employees should review their records on an annual basis, if not more often. See the Records Management Operations Policy on CIBERspace for more information.

### **Doing Business with the Government**

Special care must be taken when dealing with federal, state and local government clients. Activities that might be appropriate when working with private sector clients may be improper and even unlawful when dealing with government employees. For example, under the federal Procurement Integrity Act, it is generally unlawful for CIBER employees to discuss employment or business opportunities with any government official involved in a pending procurement; to solicit or obtain certain types of information from the government employee; work or consult on a proposal for a contract where that employee was involved in the procurement as a government employee during the preceding year.

The law also strictly prohibits offering or giving anything of value to a government employee involved in a pending procurement. CIBER policy 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.

Federal law prohibits offering, soliciting or accepting any kickback, as well as including any kickback amount, in a contract with the United States. The prohibition on kickbacks applies to both government and contractor employees. CIBER's employees may not solicit, accept, offer, or give anything of value, including money, fees, tickets, commissions, credit, gifts, gratuities, property, or compensation of any kind, for the purpose of obtaining or rewarding favorable treatment in connection with a CIBER contract or subcontract. The provision of anything of value can result in CIBER being disqualified from bidding for government procurement contracts. As employees interact professionally and socially with government employees, they must avoid even the inference that any act was intended to obtain favorable treatment under our contract. A gesture intended to promote good will may have the opposite effect by making the recipient uncomfortable about having to turn down (and possibly report) the offer. There is no minimum standard of value under the law – anything of value, no matter how small, may give rise to a violation.

In addition, federal criminal and civil laws and regulations prohibit or restrict employment discussions with certain current government employees. They also prohibit permanently, or limit for certain periods of time, the type of work that may be performed by a former government employee. Because these laws and regulations change periodically, the Law Department should be consulted before responding to or initiating any contact with a government employee concerning present or future employment opportunities.

Any questions regarding application of this policy to state and local government officials should be directed to the General Counsel, CIBER Law 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 Law Department will ensure that the reporting requirements of these laws are accomplished.

### **Foreign Corrupt Practices Act**

The Foreign Corrupt Practices Act (“FCPA”) prohibits CIBER employees from offering, paying, promising to pay money or give anything of value, directly or indirectly, to officials of any foreign government, candidates for foreign political office, or foreign political parties or party officials (collectively “Foreign Officials”) for the purposes of obtaining, retaining or directing business.

Under the FCPA, there are two very limited circumstances pursuant to which a person may provide money or something of value to Foreign Officials. Questions about these exceptions should be directed to the Law Department.

### **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. Under federal law, CIBER may not contribute corporate funds or make in-kind corporate contributions to candidates for federal office and no employee or agent may approve such contributions on behalf of the Company. In those states that prohibit contributions to state political candidates, CIBER's policy is the same as that for federal candidates. 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 Law Department.

Because lobbying and lobbyists are regulated by the law, employees may not engage in lobbying on behalf of the Company or engage others to do so unless specifically requested to do so by an elected officer of the Company in consultation with the Law Department.

In addition, federal law prohibits the recipient of a federal contract, grant, loan, or cooperative agreement from using appropriated funds to pay anyone for influencing or attempting to influence government or congressional personnel in the awarding or modifying of any federal contract, grant, loan, or cooperative agreement. The law also requires the recipient to furnish a declaration consisting of a certification and a disclosure during the procurement process. Extreme care should be exercised to ensure appropriated funds are not used for any prohibited lobbying activities. Any suspected violations should be reported to the Chief Financial Officer, Chief Accounting Officer or the General Counsel.

### **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. CIBER considers 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.

The Company has 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. Employees must justify to their supervisor the selection of alternative vendors before purchasing products and services from them.

Employees may not request gifts or entertainment that may influence their 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 the Company and is not an employee.

Employees and their immediate family members and other individuals living in their 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 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.

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

Promptly return unacceptable gifts to the supplier. If return is impractical (such as perishable fruit, etc.), donate the gift 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.

### **Client Relationship**

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

CIBER employees compete vigorously, but fairly. CIBER does not misrepresent its 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. CIBER communicates clearly and precisely so that our clients understand the terms of our contracts, including performance criteria, schedules, prices, and responsibilities.

### **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, or hiring a consulting company to engage in any of this conduct. There are also other ways competitive information could come to an employee's attention, such as when they are attending trade shows, trade association gatherings, or other types of meetings with competitors. In such cases, CIBER employees 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 a CIBER employee 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 the antitrust laws. If employees find themselves involved in this type of discussion, excuse yourself and immediately report the incident to the Law Department.

### **Intellectual Property**

All work done at CIBER or CIBER's clients shall be "work done for hire." CIBER's work is predominantly for the benefit and ownership of our clients. Any and all inventions, discoveries, concepts, improvements, processes, methods, tools, utilities, etc., whether or not subject to patents, copyrights, trademarks, or service mark protections, and whether or not conceived, developed or created by a CIBER employee while working for CIBER or its clients that relate to or result from the actual or anticipated business, work, research, or investigation, shall be the sole and exclusive property of CIBER or its clients, not of such employee(s), and no employee shall assert any patent or copyright for such work. The employee agrees to assign to CIBER, or its designee, any rights they may acquire in such inventions as they are created, throughout the

world, in perpetuity. CIBER's employees will assist CIBER and its clients in the enforcement of such matters, including signing further documentation, if and as requested, to assure all produced or in-process work belongs to CIBER or its clients. Employees shall turn over to CIBER or its clients immediately upon request one hundred percent of all confidential materials, software and other tangible and intangible property related to work performed for CIBER or its clients, whether on a client site or elsewhere.

### **Communications with the Financial Community and Media**

The Company has designated certain spokespersons as the only employees who can discuss certain information with the news media and financial community.

#### *Communications with the Financial Community*

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

#### *Communications with the Media*

An employee receiving a call from an editor/reporter representing local newspapers, TV/radio stations or other business/financial publications should refer the caller to the Director of Investor Relations or the Vice President of Marketing 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/finance.

#### *Communication via the Internet*

Employees must be very careful when participating in Internet communications, such as chat lines or message boards. Do 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.

#### *Other Requests for Information*

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

### **Contract Authorizations**

CIBER's board of directors has delegated to certain individuals the authority to sign contracts and other agreements and to legally bind the Company to those contracts and agreements. Unless employees are one of those individuals to whom such authority has been delegated, they should not sign any contracts or agreements. CIBER's policy on Contract Approval identifies who may sign contracts and at what dollar levels.

## **Harassment and Non-Discrimination**

In accordance with applicable law, CIBER prohibits sexual harassment as well as any harassment because 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. All such harassment is unlawful and will not be tolerated.

### 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 employment 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 working 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.

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.

### Prohibition of Harassment

An employee of CIBER, whether a coworker or manager, who is found to have engaged in prohibited 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. CIBER does 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, CIBER reserves the right not to provide a defense or pay damages assessed against employees for conduct in violation of this policy.

### Complaint Procedure

CIBER's complaint procedure provides for an immediate, thorough, and objective investigation of any claim in violation of this policy and appropriate disciplinary action against one found to have engaged in harassment.

If an employee believes they have been harassed on the job, or if they are aware of the harassment of others, they should provide a written or verbal complaint to their manager or to any other manager or to the Director of Human Resources as soon as possible. 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 documentary evidence (notes, pictures, cartoons, etc.). All incidents of harassment that are reported will be investigated. CIBER will immediately undertake or direct a thorough and objective investigation of the harassment allegations. In conducting an investigation CIBER will endeavor to communicate information only to those in a need to know capacity, however CIBER cannot guarantee confidentiality.

The investigation will be completed and a determination regarding the reported harassment will be made. If it is determined that harassment has occurred, CIBER will take remedial action commensurate with the circumstances, up to and including termination. Appropriate action will also be taken to deter any future harassment.

Applicable law also prohibits retaliation against any employee by another employee or by CIBER for using this complaint procedure or for filing, testifying, assisting, or participating in any manner in any investigation, proceeding, or hearing conducted by a governmental enforcement agency. Additionally, CIBER will not knowingly permit any retaliation against any employee who complains of prohibited harassment or who participates in an investigation.

### **Workplace Safety**

The health and safety of employees and others on Company property or assigned to client sites are of critical concern to CIBER. We strive to attain the highest possible level of safety in all activities and operations. CIBER also intends to comply with all health and safety laws applicable to our business.

To this end, CIBER must rely upon employees to ensure that work areas are kept safe and free of hazardous conditions. Safety is every employee's responsibility. All employees should inform their supervisor about any potential hazards and do everything reasonable to keep CIBER a safe place to work. Work-related injuries should be reported to management in accordance with the Worker's Compensation policy described in the Employee Benefits section of the Employee Handbook.

### **Compliance with this Code**

CIBER believes strongly in ethical behavior and encourages compliance with this Code by all employees. People who work together for a common purpose benefit from being aware of the guidelines pertaining to their conduct and relationships. Violations of the Code should be promptly reported to the CIBER Law Department.

The following list is based on the requirements of this Code and includes some, but not all, inappropriate employee conduct that would result in disciplinary action.

- 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 which may endanger the well being of any employee or company operations
- Use of company materials, time or equipment for unauthorized purposes
- Taking advantage of business opportunities that reasonably should be CIBER's

- Misuse of CIBER or client confidential information
- Engaging in practices that are inconsistent with ordinary and reasonable rules of conduct necessary for the welfare of the Company and its employees
- Willful or repeated violation of Company rules
- Violation of client policies

Employees who do not comply with provisions of this Code or other CIBER or client policies or procedures will be subject to corrective action that could include a broad range of disciplinary action, from informal counseling, up to and including, termination of employment. Disciplinary action may also include legal action and/or referral to a government agency. Disciplinary action will be structured on a case-by-case basis.

### **Questions and Resources**

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

- Employees immediate supervisor
- A more senior manager in employees business unit
- CIBER's Director of Human Resources at CIBER's Corporate office- 800-242-3799
- CIBER's General Counsel at CIBER's Corporate office- 800-242-3799

In addition to the individuals listed above, if employees have concerns about the Company's accounting, internal accounting controls and auditing matters, they may address their complaint or concern to the Chairman of the Company's Audit Committee by sending their concern via email to [auditcommitteechair@ciber.com](mailto:auditcommitteechair@ciber.com) or via U.S. mail to Chairman of the Audit Committee, CIBER, Inc., 5251 DTC Parkway, Suite 1400, Greenwood Village, Colorado 80111.