VERITIV CORPORATION

CODE OF BUSINESS CONDUCT AND ETHICS

(Effective as of December 15, 2020)

Message from the CEO

Dear Veritiv Team,

Integrity is an essential element of our corporate culture. We place a high value on honesty, fair dealing and ethical business practices. No one employed by Veritiv Corporation or our affiliates should ever compromise sound standards of ethical behavior. Our continued success and corporate reputation rely on maintaining the exceptional standards that our employees demonstrate every day.

A cornerstone of this vision is the **Veritiv Code of Business Conduct and Ethics**. The Code guides each of us on the standards of conduct that support the Veritiv Values and govern our business. The Code provides direction and a framework to ensure we act ethically, responsibly and in compliance with the law.

Our senior leaders, including our board of directors, support this Code and are committed to keeping its values and principles at the core of our operations. Each of us has a responsibility to be well informed about the Code and ensure we are exercising good judgment as we conduct our business.

Doing the right thing can be difficult at times. We count on all of our employees to not only adhere to this Code, but to report any violations. We respond to all reports regarding violations of the Code, and we will not tolerate retaliation against any employee who raises a concern in good faith.

Veritiv's reputation and success are in each of our hands. We must strive to demonstrate fairness, integrity, professionalism and honesty as we make decisions and conduct business daily. In doing so, we will contribute to the success of our customers, suppliers, shareholders and each other.

Thank you for your continued commitment to ethical and legal behavior, and to living our Veritiv Values every day.

Regards,

Salvatore A. Abbate
CEO

TABLE OF CONTENTS

INTRODUCTION

Scope

This Code of Business Conduct and Ethics (the/this "Code") applies to all employees and the members of the Board of Directors (collectively "employees") of Veritiv Corporation and/or its subsidiaries and affiliates (each individually and together collectively referred to herein as "Veritiv" or the "Company").

This Code confirms the basic elements of honesty, integrity, fairness, responsibility, professionalism and good judgment that all Company employees are required to observe. A basic principle of this Code is that employees must always act lawfully and refrain from taking any action that violates the letter or spirit of any applicable law or regulation. While not a comprehensive rulebook, the Code is a statement of the way that the Company does business, reflecting the Company's core values and commitment to "doing the right thing" in all that employees do.

Compliance

Compliance with the Code is mandatory. Illegal or unethical conduct cannot be justified by claiming that it benefited the Company or was directed by a higher authority within the organization. No one at the Company is authorized to conduct themselves or direct others in a manner inconsistent with the Code. Likewise, employees may not use other employees or contractors, agents, consultants, family members or other third parties to perform any act prohibited by the Code. Employees who violate the Code will be subject to appropriate disciplinary action. Nothing in the Code changes the fact that, unless prohibited by law, all Company employees are employees at will.

Administration

The Board of Directors has delegated authority to the Company's Legal Department to administer the Code, including investigating reported or suspected violations of the Code, determining whether any violation has occurred and implementing disciplinary action, if appropriate. Notwithstanding the foregoing, any waiver of the Code for executive officers or directors may be made only by the Board of Directors or the Nominating and Governance Committee.

Modification and Interpretation

The Company reserves the right to modify, terminate or replace this Code at any time. Any questions relating to how the Code should be interpreted or applied should be addressed to the General Counsel or Chief Compliance Officer. Interpretations of this Code will be at the sole discretion of Veritiv management and all such interpretations will be final and binding. ***See the Contact List at the end of the Code.***

Training and Attestation

Employees will receive training on the Code in accordance with Company policy and procedure as established from time-to-time by Veritiv management. All employees will be required to attest that each has received this Code, has read and understood it, and has agreed to abide by it as required by Veritiv management and applicable Company policy and procedure.

Conflict with Other Policies

This Code does not include every Veritiv policy and is not intended to replace other existing, or hereafter instituted, Veritiv polices. To the extent a specific Veritiv policy addresses the same or similar subject matter referenced in this Code, the provisions of the more specific policy shall control.

Expectation of Employees

Employees are expected to exercise due care in connection with the performance of the responsibilities and duties of their employment position with the Company.

Audits, Investigations and Disciplinary Action

Compliance with this Code may be monitored by periodic audits, which may or may not be announced in advance. Unless contrary to applicable law, all employees are required to cooperate fully with any such audits, as well as with any investigation of reported or suspected wrongdoing and with any disciplinary or remedial action imposed by the Company. In addition, employees are required to provide truthful, accurate information and to respond to requests for certifications in connection with audits, investigations and remedial actions initiated by the Company. Failure to comply with any of these requirements may lead to disciplinary action.

Reporting Violations

All employees must report situations that could result in violations of federal, state or local laws; the principles, policies or procedures set forth in this Code; or any other Company policies or procedures. Failure to do so may lead to disciplinary action. Confidential reports should be directed to the reporting employee's direct-line management, the Human Resources Department, and/or Legal Department. Employees may also file reports by calling the Company's HelpLine (888- 312-2693 in U.S. and Canada; in Mexico 800-462-4240 and then dial 877-556-5341); or emailing to http ://veritivhelpline.com. Calls or emails to the HelpLine provide the opportunity to identify yourself or to remain anonymous. ***See the Contact List at the end of the Code.***

No Retaliation

Employees will not be penalized for good faith reporting of suspected violations of this Code or any other Veritiv policy or for cooperating with any Company investigation. Retaliation or threats of retaliation, against any employee who reports a possible violation or who cooperates with any Company investigation will not be tolerated.

Collective Bargaining Agreements

For employees covered under a collective bargaining agreement, if there is a conflict between the provisions of this Code and the collective bargaining agreement, the collective bargaining agreement will control to the extent of such conflict.

POLICIES

1.0 FOSTERING A SAFE AND RESPECTFUL WORKPLACE

1.1 Equal Employment Opportunity

Veritiv is proud to be an equal opportunity employer and is committed to providing equal employment opportunities to all employees and employment applicants without regard to any classification protected by law as detailed in the Veritiv Equal Employment Opportunity Policy which is posted at each facility and available on the Veritiv intranet.

1.2 Freedom from Harassment

The Company promotes a workplace culture of dignity and respect for all employees as well as a safe, appropriate, and productive work environment. Accordingly, the Company prohibits unlawful harassment and discrimination at Company work facilities, as well as off-site business trips, business functions, and/or Company-sponsored events, or where otherwise representing the Company. The Company also prohibits any form of degrading, offensive, or intimidating conduct based on a person's classification protected by law as detailed in the Veritiv Equal Employment Opportunity Policy.

Every employee is required to follow our policies against unlawful discrimination and harassment and to bring to the Company's attention any action that does not comply with those policies or our commitment to equal employment opportunity. Supervisors and managers must be watchful for any signs that these policies are not being followed and must see that any possible violations are immediately referred for investigation, whether or not there has been a formal complaint. Veritiv does not tolerate threats or acts of retaliation or retribution against employees who make good faith use of the complaint procedures or who provide information about such complaints.

1.3 Workplace Safety

Veritiv's operations will be managed to protect the health and safety of its employees and the communities where it does business. Safe operating practices will be followed to foster a safe working environment. We not only operate our facilities according to applicable health and safety laws, but we also use risk identification to focus on eliminating or mitigating those tasks that could cause harm, and we communicate such information across the Company to improve overall safety performance. We may also have policies that are stricter than the law. For example, we expect accurate and timely reporting of safety incidents, regardless of whether they trigger any regulatory reporting. We also require every Company facility to have a safety program in place.

Many of Veritiv's safety rules in the United States are based on legal requirements of the Occupational Safety and Health Administration (OSHA) and the Federal Motor Carrier Safety Administration, as well as state law requirements and the laws of other countries in which Veritiv facilities are located.

Our co-workers, communities, customers and shareholders all expect us to work safely, and our policies require it. We do not tolerate any verbal or physical conduct that could lead to violence. For the security and well-being of all, our employees must work free from the influence of any substance or activity that would threaten the safety of our work.

All of us are responsible for our own safety and that of our coworkers. Therefore, the Company encourages employees to be proactive with regard to the development of safe work practices, to identify,

correct and report potential workplace hazards, and to help prevent accidents by increased awareness in the workplace and the active reporting of near-miss incidents so that corrective actions can be applied before actual accidents occur.

Employees are also required to bring to the Company's attention any violation of our safety policies and procedures. Retaliation against those who report violations in good faith will not be tolerated.

1.4 Employee Privacy

Employees should have no expectation that communications at work or using Company facilities will be private. The Company has the right to monitor or review workplace communications, including Internet, e-mail, telephone and voicemail communications, for any reason, with or without notice, subject to applicable laws. The Company also has the right to search employees' workspaces at any time, for any reason, with or without notice, subject to applicable laws.

2.0 MAINTAINING ETHICS AND INTEGRITY IN BUSINESS ACTIVITIES

2.1 Compliance with Laws and Regulations

The laws of many jurisdictions impact Veritiv's operations. These laws include not only those of the United States, Canada and Mexico or other country, state or locality in which Company operations are located, but also those of other countries in which the Company conducts business. Veritiv's employees must comply with such laws and regulations, even if its competitors, suppliers or customers may choose not to do so.

2.2 Unfair Trade Practices; Malicious Deception and Fraud

In our highly competitive marketplace, Veritiv will achieve a competitive advantage on the basis of price, quality and service. While the Company needs to aggressively pursue business, employees must do so within the confines of ethical business practices and applicable laws. No illegal or unethical activity to obtain business, including offering bribes or kickbacks, is ever acceptable.

Accordingly, employees must not engage in any form of unfair, fraudulent or maliciously deceptive practice against the Company or any customer, supplier, co-worker, competitor or any other third party. Employees should never create intentionally misleading impressions, omit important facts or make false claims about our offerings or those of our competitors.

A malicious misrepresentation to the Company is a form of intentional deceit and is strictly forbidden. Examples of such misrepresentations include the submission of falsified expense reports for the purpose of obtaining reimbursement payments for expenses not truly incurred.

Other prohibited business practices include forgery and interference with contractual relations. Employees should never sign any business or legal document, such as a customer or supplier contract, on behalf of a customer, supplier or any other party. Employees also are not permitted to interfere with a competitor's contractual or business relationships, for example, by urging a customer or potential customer to breach its contract with the competitor. Employees should never offer legal advice regarding any competitor's contract.

2.3 Bribery and Inappropriate Gifts

Employees are prohibited from engaging in any form of commercial or governmental bribery or otherwise providing gifts to others for inappropriate purposes. This means employees may not give or offer money or anything else of value to anyone with whom the Company does business or who might do business with the Company, if the purpose of the gift is to encourage that person to do something corrupt, deceptive or otherwise opposed to that person's legal or ethical obligations or responsibilities. Similarly, employees are not permitted to give or offer money or anything else of value to anyone with whom the Company does business or who might do business with the Company if it is intended to directly impact their judgment with respect to a business decision. ***See Section 4.2 of this Code for further clarification of what constitutes inappropriate gifts.***

2.4 Safeguarding Confidential Information of Others

The Company's policy is to respect Confidential, Proprietary, Privileged, and Secret Information (CPPSI, as defined below) of others. This includes information about devices, inventions, proprietary procedures, product specifications, customer or supplier lists, pricing lists or information, marketing or business plans, business strategies and results, proprietary operational procedures, technical, design or process data, acquisition or teaming plans, proprietary project practices, trade secrets, know -how, and private personnel data of other individuals learned through special authorized access to such information such as medical information, banking information, social security numbers, etc. (collectively referred to as CPPSI). Liability for the unauthorized use of others' CPPSI can be significant. Accordingly, employees should contact the Legal Department immediately if they believe that the confidential information or intellectual property rights of others are being misused or violated.

During the course of employment, employees may gain access to, or otherwise become aware of, the CPPSI of the Company's customers, suppliers, business partners or other parties. Employees may not use this information or property for any purpose unrelated to the products or services provided by the Company as authorized by the customer, supplier, business partner or third party without first obtaining the advice and consent of the Legal Department. In addition, no employee may divulge such information or provide such property to anyone outside the Company unless authorized to do so by the Company consistent with its obligations to the owner of that information or property.

Employees are prohibited from unlawfully obtaining or accessing any CPPSI from customers, suppliers, business partners or competitors. Unlawful means of obtaining information of others include, but are not limited to, burglary, wiretapping, misrepresentation of identity and the hiring of others for the purpose of improperly obtaining such information. The CPPSI of customers, suppliers or competitors (including voice and digital data) must not be copied, accessed, recorded, covertly listened to, or divulged without prior written approval from the participants involved in such communications, unless authorized by applicable law. Employees should avoid involvement in any situation in which CPPSI has been improperly obtained or accessed from any other company. If any employee is approached with any offer of CPPSI that the employee has reason to believe may have been obtained improperly, the employee must notify his or her manager immediately and seek advice from the Legal Department.

2.5 Document Creation and Retention

Business records and communications may become subject to public disclosure in the course of litigation or governmental investigations. In some cases, business records and communications are discoverable and can be obtained by outside parties or the media. Employees therefore should attempt to be as clear, concise, truthful and accurate as possible when creating any communication on behalf of the Company,

whether in written or electronic form. Avoid exaggeration, profanity, guesswork, legal conclusions and derogatory characterizations of people, other companies or their motives. This policy applies to communications of all kinds, including e-mail, voice mail, and "informal" notes or memos.

Documents and records must be retained for the periods of time specified by the Company's records-retention policies. Employees aware of an imminent or ongoing investigation, litigation, audit or examination initiated by the Company, any government agency, a customer or other third party, should notify his or her manager and contact the Legal Department for instructions on retaining any related documents. Should an employee be notified that a document or record has been placed on legal hold by the Legal Department, he or she is required to fully comply with the instructions stated in the legal hold notice. For additional guidance regarding administration of Veritiv's Record Retention Policy, including questions as to whether a document should be destroyed, see the Veritiv Record Retention Operating Procedures.

2.6 Falsification of Books and Records

Employees are expected to maintain accurate and reliable financial books and records at all times. All reports and assertions made to the Company including any record keeping entered into accounting books or information provided in reports, both written and verbal, must be accurate and honest. Employees are prohibited from making any false or misleading book and systems entries or reports to the Company, its management, investors, regulators, or other parties. This applies to any and all public disclosures including disclosures in investor reports, transaction documents, and public communications, as well as internal disclosures including customer orders, personal expense reports, and responses to management inquiries.

All of the Company's funds and other assets and all its transactions must be properly documented, fully accounted for and promptly recorded in the appropriate books and records of the Company, in conformity with generally accepted accounting principles ("GAAP") and the Company's system of internal accounting controls. Federal securities laws require that the Company's books and records accurately reflect all transactions, including any payment of money, transfer of property, and furnishing of services. The term "books" generally refers to the documents and records of the Company containing accounting, inventory, financial, securities and corporate business information, and the term "records" generally refers to information recorded by the Company, including time reports, sales transactions, purchasing and shipping documentation, permits and licenses, expense account records, claims reports and records, employee files and records, authorization and approvals, and other business documents and reports.

Veritiv employees are required to observe the following:

- *False books and records*. False or misleading entries shall not be made in the Company's books or records for any reason. Examples of false or misleading entries include making records appear as though payments were made to one person when, in fact, they were made to another, submitting expense reports that do not accurately reflect the true nature of the expense, and the creation of any other records that do not accurately reflect the true nature of the transaction.
- *Undisclosed assets*. Undisclosed or unrecorded funds or assets ("slush funds") or similar funds or accounts are prohibited.
- *Use of assets for unlawful purposes*. Company funds or other assets may not be used for any purpose that is unlawful. The Company will not provide services that are unlawful.
- *Undisclosed purposes*. No payment on behalf of the Company will be approved or made with the intention or understanding that any part of such payment is to be used for any purpose other than that described by the documentation supporting the payment.

2.7 Accounting, Auditing and Public Reporting Matters

The Company is committed to ensuring that the highest legal and ethical standards are utilized in the preparation and public reporting of all financial and non-financial information regarding the Company. In that regard, the Company's management encourages any employee who has any concerns regarding any procedure, policy, action, or inaction related to accounting, auditing or the Company's public disclosures to report those concerns to any of the following: Chief Financial Officer; General Counsel; Chief Compliance Officer; Head of Internal Audit; the Company's Disclosure Committee; or the HelpLine. Any such reports may be made anonymously.

Misrepresentation of material financial or non-financial information or other questionable accounting or auditing practices may result in fraudulent, incomplete, inaccurate or untimely reporting, including intentionally misleading financial statements or other material disclosures about the Company. Accordingly, employees must not undermine the integrity of any information within the reporting chain and shall not fraudulently influence, coerce, manipulate, or intentionally mislead any internal or independent auditor during the course of any audit or their procedures.

The United States securities laws also prohibit certain, selective disclosures of material non-public information about the Company. Accordingly, we have established a centralized disclosure system and have designated a limited number of Company spokespersons who are authorized to speak publicly on the Company's behalf and otherwise provide public disclosures regarding the Company. Therefore, unless so designated, employees may not speak on the Company's behalf or disclose CPPSI, and employees must forward all press or investment community inquiries requesting comment on behalf of the Company to Investor Relations. ***For more information, see Communications Outside of the Company below.***

3.0 COMPETING FAIRLY

3.1 Competition Laws

In most countries in which we operate, strict laws are in force prohibiting business arrangements that limit competition. These laws define acceptable behavior for competing in the marketplace. The general aim of these laws is to promote competition and let businesses compete fairly on the basis of quality, price, service and other valid business criteria. Failure to follow these complicated laws can mean significant penalties, both to the Company and to individual violators. We are committed to complying with the letter and the spirit of these laws and will not tolerate any business conduct that violates them.

Antitrust laws generally prohibit agreements or actions that might eliminate or discourage competition, bring about a monopoly, artificially maintain prices or otherwise illegally hamper or distort normal commerce. This means employees must pay careful attention to possible anti-competitive implications of the Company's business activities. The antitrust laws are complex, and the Legal Department should be consulted in all cases of doubt.

3.2 Dealing with Competitors

Competitors are not permitted to agree among themselves on their respective prices or terms of sale, or to divide territories, suppliers or customers among themselves. Some of the arrangements with competitors that generally are illegal under the antitrust laws are agreements fixing prices, agreements allocating territories, suppliers or customers, customer or supplier boycotts or refusals to deal, and unlawful disclosures of competitive bids. Competitors also should not agree to limit or fix the terms of employment for potential employees.

If employees are asked by a competitor to enter into an illegal or questionable agreement regarding pricing, customers, suppliers, territories or any other terms or conditions of sale, they should do all of the following:

- inform the competitor that such discussions may be inappropriate and illegal;
- immediately cease, or remove themselves from, those discussions and tell the competitor never to discuss the subject with them again; and
- immediately inform their manager and the Legal Department of the incident.

3.3 Dealing with Customers and Suppliers

Agreements with customers or suppliers that create antitrust concerns include certain exclusive dealing and/or reciprocity agreements and tying arrangements. Tying arrangements typically involve requiring the purchase of one product or service to the purchase of another, distinct product or service. Any transaction potentially involving exclusive dealing, reciprocal, or tying arrangements must be reviewed and approved in advance by the Legal Department.

3.4 Other Anti-Competitive Practices

Other potentially illegal anti-competitive practices which must be avoided include:

- *Predatory Pricing* - Setting pricing below cost with the aim of forcing competitors out of a market.
- *Disparagement* – **Maliciously** false or misleading statements critical of competitors or others.
- *Interference with the Contracts of Competitor* - Urging or suggesting that a customer or prospective customer break a contract with a competitor.
- *Price Discrimination* - Charging competing customers different prices for the same product to substantially lessen competition. Under specific circumstances, the Company may adjust its pricing offerings without creating a discriminatory pricing situation. Please check with the Legal Department for more information.
- *Monopolization* - It is illegal for a company to monopolize or attempt to monopolize a market, *i.e.*, to dominate a market by anti-competitive methods. Therefore, all employees should avoid any conduct which could be construed as an attempt to monopolize.
- *Wrongful Participation with Trade Association* – In an order to avoid claims of Company involvement in unlawful price fixing, or other anti-trust violation no employee should participate in, or remain present at, any discussion among competitors at a trade association meeting, or other gathering of association members or participants, concerning: prices or factors that determine prices; costs; credit terms or other terms or conditions of sale; profits or profit margins; allocation of territories among competitors or potential competitors; allocation of customers or suppliers among competitors or potential competitors; or a refusal to deal with customers or suppliers. Also, employees should not participate in any association meetings that hold discussions which set restrictions on competitors who are non-members of the association or set policies or practices that may harm competitors that are non-members. If an employee becomes aware of such a discussion at a trade association meeting, the employee should leave the meeting immediately and insist that his or her departure be noted in the minutes (if minutes are being recorded), and immediately advise his or her manager and the Legal Department.

3.5 Social Discussions and Company Communications

The practices outlined above do not have to be covered by formal or written agreements to be illegal. Any kind of casual understanding between two companies or even social conversations can be used as evidence that an agreement existed. Business memos and other written business communications that use casual non-professional language might someday be examined by a government agency or opposing lawyer. Using loose language may raise questions about conduct that is entirely legal and may undermine what otherwise would have been successful efforts to comply with the antitrust and competition laws.

4.0 CONFLICTS OF INTEREST; GIFTS AND ENTERTAINMENT

Employees must avoid any action, investment, interest or association that reasonably might interfere, or appear to interfere, with their independent exercise of judgment in the best interests of the Company and its stockholders. Conflicts of interest often arise when an employee's position with the Company presents an opportunity for personal gain apart from the normal compensation provided through employment.

4.1 Transactions Presenting a Conflict of Interest

Any situation that creates - or even appears to create - conflict between personal and Company interests must be avoided, resolved or reported. If an employee finds himself or herself in a relationship or activity that might pose a conflict of interest, the employee must disclose it to his or her manager or the Legal Department and get written approval before proceeding. In some cases, disclosure cannot resolve the conflict, in which case the employee will have to take steps to remove it. (See guidelines below for examples of conflicts of interest).

An employee should not have any position with, or substantial interest in, any business enterprise, the existence of which would conflict or might reasonably be supposed to conflict with the proper performance of the employee's Company duties or responsibilities, or which might tend to affect the employee's independent judgment with respect to transactions between the Company and such other business enterprise.

To help you better understand what types of activities are considered to be a "conflict of interest," the following guidelines apply to most common conflict situations:

Employment/ Positions with Outside Companies.

- For all full-time Veritiv employees, employment with Veritiv must be the first priority. Any outside employment, investment or other source of income must be secondary and must not interfere with the performance of the employee's duties as a Veritiv team member. Full-time Veritiv employees may not work in any capacity for another company that competes with the Company or any of the goods and services the Company provides. Full-time Veritiv employees may work for other companies that do not provide or seek to provide goods and services to the Company, provided: the hours and responsibilities for the other company do not conflict with the required working hours (including overtime) or have a negative impact on your work required by the Company; no Company assets can be used to conduct the work for the other firm; and involvement with the other company does not create any negative connotations or images for the Company.
- A full-time Veritiv employee may not serve as an officer, director, partner, employee or consultant of, or otherwise work for, a vendor, supplier, customer or competitor while working for Veritiv.

- A full-time Veritiv employee may serve as a director or officer of an outside company only in the following circumstances unless otherwise required by law: as a director or officer of non-profit organizations such as church groups and charities; and as a director or officer of a for-profit organization only after receiving written approval by the Company's CEO and General Counsel. While serving as an officer or director of any organization other than a labor union, the employee shall abstain from any votes or decisions that involve the Company, any type of business or industry in which it is engaged, or any of its competitors.
- A manager should not hire a current Company employee to work as a consultant or other independent contractor for the Company where payment is made outside normal payroll procedures. This applies without exception, regardless of whether or not the work is related to the duties of the employee's position. Former employees may be retained by the Company as consultants only under certain, Company-prescribed circumstances and must be approved by the Human Resources Department.
- The Company maintains strict policies regarding the employment of relatives to ensure that employees are acting in the best interest of the Company. No relative of an employee may report directly or indirectly to his/her relation. Relatives include, a person's spouse, parents, children, siblings, grandparents, uncles, aunts, nieces, nephews, in-laws, and anyone (other than domestic employees) who shares such person's home. This definition applies to both blood relatives and relatives by marriage or adoption. It is each employee's responsibility to fully disclose the identity of any applicant or current employee who falls within the definition of a "relative" as described in this Code. Members of the Veritiv Senior Leadership Team must disclose to the General Counsel and the Chair of the Audit and Finance Committee of the Board of Directors the identity of any applicant or current employee who falls within the definition of "relative" as described in this Code.

Finances

- An employee may not loan money to or borrow money or accept monetary gifts from individuals or organizations that do business with or compete with Veritiv.
- An employee may not buy or sell goods or services on behalf of Veritiv from or to any company in which such employee or a close family member may personally benefit from such purchase or sale without full disclosure to such employee's manager and approval from the CEO and General Counsel.

Business Opportunities

- An employee should not make any investment that might affect his or her business decisions. For example, employees may not own or have a significant interest in a company that is a competitor or one that has current or prospective business with Veritiv. This prohibition does not apply to owning less than one percent of the stock of a publicly traded company.
- Any investment of more than five percent of an employee's investment portfolio, and any relationship with an employee's family members, is presumed "significant" under this Code. Any interest in another company that reasonably could influence an employee to make a decision based on that company's or the employee's own interests rather than the Company's best interest is considered "significant." An interest can be financial, such as owning stock, or personal, such as a family or other close relationship with an owner of a company.
- Employees are also prohibited from directly or indirectly bidding for, purchasing, leasing or otherwise acquiring any property or asset or pursuing a business opportunity if they are aware or should be aware that the Company may also be interested in acquiring the same.

Employees are required to disclose to the Company any actual or potential conflicts of interest they may have under the guidelines described in this Code. In the event of conflicts that arise during the course of employment, employees are required to promptly report such conflicts to his or her manager or a representative of the Legal Department or by contacting the HelpLine (888- 312-2693 in U.S. and Canada;

in Mexico 800-462-4240 and then dial 877-556-5341) or http://veritivhelpline.com.

4.2 Gifts and Entertainment

Gifts and entertainment are a common way we create goodwill and strengthen our business relationships, but they can also make it difficult to make objective decisions about business partners. In some cases, providing business gifts and entertainment may even be illegal, such as when the recipient is a government official. For these reasons, employees should avoid their use if they will create even the appearance of compromising business decisions. This is the case whether the employee is the giver or recipient. Maximum values for gifts are established as part of the Veritiv Gift Policy and are updated annually. Employees should consult the Veritiv Gift Policy located on the Veritiv intranet for additional guidance.

What is Allowed. It is generally allowed to give or accept entertainment or gifts of nominal value that are:

- reasonable in value and customary;
- given openly and transparently;
- given to promote legitimate business relationships;
- properly recorded according to Company accounting requirements; and
- tasteful and commensurate with Veritiv's commitment to treat everyone with respect and dignity.

What is Not Allowed. Employees should never accept gifts, favors or entertainment when doing so obligates them - or even *appears* to obligate them - to the giver. Nor should employees give any gift or provide entertainment with an expectation that the receiver will be obligated to him or her. Employees should never give or accept gifts that are lavish, repeated or could be interpreted as bribes - *even when acceptable by local custom.* Employees should not give or accept cash or gifts that work like cash, such as gift cards. Similarly, nobody working for the Company should request gifts, services or contributions from vendors, suppliers or other business partners - whether for personal benefit or on Veritiv's behalf. Such requests are only allowed on behalf of charitable organizations that the Company officially supports. Always seek the advice of the Legal Department before you give any form of gift or entertainment to anyone affiliated with a government or government-controlled company.

Government Officials. Rules for dealing with federal, state and local governments differ from those applicable to dealing with other customers. Something that is considered a normal business courtesy in the commercial marketplace can be considered an attempt to improperly influence a government official. Accordingly, Veritiv employees are not permitted to offer, give or promise to give anything of value to a government employee or their immediate family members.

Respecting Local Standards. Some departments - and even some countries - may have stricter guidelines on giving and receiving gifts, and special procedures may apply in certain situations. Employees are responsible for knowing the standards that apply to them.

5.0 DOING BUSINESS WITH SUPPLIERS AND VENDORS

5.1 Suppliers Generally

Veritiv selects suppliers based on objective criteria such as the quality and cost of their goods and services, and also seeks suppliers that demonstrate high standards of ethical business conduct. The Company will do business only with suppliers and vendors that embrace and demonstrate high principles of ethical business conduct and will not knowingly use suppliers who operate in material violation of applicable laws or regulations, including environmental, employment or safety laws. The Company takes steps to make sure

that its key suppliers understand the standards that we as a Company apply to ourselves and expect from those who do business with us.

5.2 Procurement Practices

Veritiv's business strategy involves partnering with suppliers, contractors, joint venture partners and other independent businesses. The Company proactively looks for partners that embrace and practice high ethical standards - and we let them know what the Company's expectations of them are. In these relationships, while the Company may not control the business arrangement, it will use its influence and leadership to help its partners maintain high ethical standards of behavior.

When making purchases of goods and services on behalf of the Company, employees are required to observe the Company's procurement practices and guidelines as established by the Company's Procurement Department.

Procurement agreements should be written to clearly identify the services or products to be provided, the basis for payment and the applicable price. The price must not be excessive in light of industry practice and must be commensurate with the services or products provided. No commitments or agreements should be made behalf of the Company without proper fiscal and signatory authority.

The Company will contract with each of its suppliers only on the basis of quality, price, service and other valid business criteria. The fact that a supplier or potential supplier may also be a customer of the Company shall not be the determining factor for making purchasing decisions. No employee may condition purchases from a supplier on the supplier's patronage with the Company, nor shall any employee attempt to persuade suppliers to purchase from the Company simply because the Company buys from them.

5.3 Contract Authorization; Letters of Intent

Any authority to execute contracts on behalf of the Company is limited. Employees executing contracts must observe the Veritiv Delegation of Authority and all current established guidelines concerning designated policies for authority and financial approvals. When conducting business on behalf of the Company, employees may execute only agreements arranged for, written by, and/or approved by the Legal Department pursuant to current guidelines. Employees are prohibited from authorizing changes to any contractual agreement terms unless approval to do such is granted by the Legal Department pursuant to current guidelines. The Company prohibits employees from issuing letters of intent unless the Legal Department grants prior approval.

5.4 Retaining Outside Legal Counsel

Outside legal counsel may be retained and directed on behalf of the Company only by the Legal Department, unless the Legal Department approves the retention by other departments or organizations of outside legal counsel for limited purposes, such as prosecuting collections actions against third parties. Employees are prohibited from selecting and obtaining their own outside legal counsel to handle business on behalf of the Company.

5.5 Environmental Protection

Our Commitment. The Company believes that being accountable means respecting, protecting and preserving the environment. Veritiv is committed to:

- supporting environmental sustainability
- using resources and energy efficiently; and
- using technology that minimizes environmental impact, where feasible and appropriate.

Employees whose work may impact the environment must be thoroughly familiar with the applicable permits, requirements and procedures associated with their jobs.

Third-Party Certifications. As part of Veritiv's commitment to the environment, the Company follows a use policy that recognizes third-party certifications related to fiber sourcing. Veritiv also works with suppliers to source and provide products certified by third-party organizations that support our customers' sustainability goals. This way, we know that we are using trees that are grown and harvested with methods that protect biodiversity, wildlife, plants, soil and water quality. We support third-party certification to globally recognized standards in the countries where we operate. We are also committed to expanding certification throughout our supply chain.

6.0 DOING BUSINESS WITH THE GOVERNMENT

6.1 Government Sales in the United States

Generally. Veritiv frequently acts as a supplier to the U.S. government and as a subcontractor to other primary government contractors. In doing business as a primary contractor or subcontractor, Veritiv must maintain strict compliance with all applicable statutes, regulations and contractual requirements. Failure to do so can lead to serious consequences, including financial penalties and criminal prosecutions. Employees engaged in business with a governmental body or agency must know and abide by the specific rules and regulations covering that entity. Such employees must also conduct themselves in a manner that avoids any dealings which may be perceived as attempts to influence public officials in the performance of their official duties.

Accuracy and Contract Compliance. Information submitted to the government must be current and accurate. Deviations from government contract specifications and requirements are not permitted without prior written approval from an authorized government official.

Receipt of Sensitive Information. Veritiv employees may not seek or knowingly obtain bid or proposal information or "source selection sensitive information" (i.e., non-public information that is prepared for use by a federal agency for the purpose of evaluating a bid or proposal) before the award of the government contract or subcontract to which the information relates.

Hiring Former Government Employees. Any discussion or contacts with current or former government employees, whether military or civilian, for the purpose of exploring potential employment or consulting opportunities with Veritiv may be subject to conflict of interest laws. Likewise, such individuals may be prohibited from certain tasks and duties once hired. Consult Human Resources and the Legal Department before engaging in any employment or consulting discussions with current or former government employees to ensure compliance with these rules.

Prohibited Relationships. Veritiv will not employ or contract with an individual or company that is debarred, suspended or otherwise ineligible to do business with the U.S. government

No Gifts, Meals or Gratuities. Rules for dealing with federal, state and local governments differ from those applicable to dealing with other customers. Something that is considered a normal business courtesy in the commercial marketplace can be considered an attempt to improperly influence a government official. Accordingly, Veritiv employees are not permitted to offer, give or promise to give anything of value to a government employee or their immediate family members.

Mandatory Disclosures. Veritiv's policy is to comply with all applicable regulations that require the disclosure of any credible evidence of a violation of federal criminal law involving fraud, conflict of interest, bribery, illegal gratuities, government overpayments or violations of the False Claims Act. If an employee learns of any such evidence or other conduct that is inconsistent with Veritiv's obligations as a government contractor or subcontractor, such employee must report it immediately to the Legal Department or by calling the HelpLine at (888) 312-2693 (U.S. and Canada); in Mexico 800-462-4240 and then dial 877-556-5341or emailing at http://veritivhelpline.com.

6.2 Doing Business in Other Countries

Generally. All countries where Veritiv operates regulate international trade transactions such as imports, exports and financial transactions. As a U.S. company, we must follow U.S. trade laws wherever we do business, even when they may be in conflict with similar laws of other countries. We will strictly adhere to those U.S. and foreign laws which regulate international trade transactions such as imports, exports and financial transactions around the world that are designed to prevent corruption and bribery, such as the U.S. Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act and certain local laws. These laws forbid our company, our employees and third parties who work on our behalf to offer of pay anything of value in order to (i) get illegal or unlawful business advantages or (ii) influence people who are making decisions that affect us.

Money Laundering Prevention Laws. Sometimes complex commercial transactions can hide funding for criminal activity such as fraud, bribery, tax evasion and illegal narcotics or weapons trafficking. Money laundering prevention laws require that payments be transparent and that all involved parties be clearly identified. At Veritiv, we comply with money laundering prevention laws all over the world, and we will only do business with reputable customers who are involved in legitimate business activities.

Export Control Laws. The United States has strict export control laws, which forbid Veritiv from exporting U.S. goods to certain people and places outside the United States. There are also some cases where the Company cannot export goods from its own operations abroad. Veritiv must also be aware of and follow the export control laws of other countries where it operates. "Exports" can be tangible items, such as paper and packaging products. There are also intangible exports, such as electronic data or other information that can be "exported" through conversations or emails. Any employee involved in exports must be aware of the applicable rules.

Anti-Boycott Laws. By law, Veritiv cannot participate in restrictive trade practices or boycotts that foreign governments impose on other countries or against U.S. citizens or companies. In fact, Veritiv cannot be part of a boycott that is not sanctioned by the U.S. government. Veritiv must not enter into any agreement, provide any information, or make any statement that might be viewed as supporting any boycott prohibited by U.S. law.

7.0 COMPLIANCE WITH SECURITIES LAWS

7.1 Insider Trading

The insider trading laws of the United States prohibit buying or selling the Company's securities while in possession of material, non-public information about the Company. These laws also prohibit disclosing material, non-public information to another person if, as a result of the disclosure, that person or any other person receiving the non-public information as the result of the prohibited disclosure buys or sells a security on the basis of that information. Any employee who makes such a disclosure can be punished under the law, even if she or he realizes no financial gain.

"Material" information is generally regarded as information that a reasonable investor would deem important in deciding whether to buy, hold or sell a security. In short, it is any information that could reasonably affect the price of the security. Examples of possible material information are sales or other financial results or issues, earnings, dividend actions, strategic plans, new products, important management or other personnel changes, acquisitions, divestitures or other similar strategic plans, marketing plans, litigation or government actions or major cybersecurity incidents.

"Non-public" means the information has not been "publicly disclosed" meaning broadly disseminated to the public. An employee who becomes aware of material information about the Company before it is publicly disclosed should refrain from trading in the Company's stock until at least two full trading days have elapsed after such information is publicly disclosed. In this context, public disclosure means the Company has included the information in a filing it makes with the Securities and Exchange Commission (the "SEC") or in a news announcement or other broadly disseminated press release. Even after material information has been publicly announced, the Company's stockholders and the public must be given a reasonable time to digest the information and act upon it. Generally, two full trading days is sufficient.

Employees may not buy or sell, or otherwise transfer, Company securities while in possession of material, non-public information. In addition, employees may not engage in any other action to take advantage of, or pass on to others, material, non-public information. This policy also applies to buying or selling securities of any other company while employees have material, non-public information about that other company that they learned during the course of their employment with the Company. These same restrictions apply to each employee's family members and others living in an employee's household. Each employee is responsible for ensuring his or her compliance with these restrictions. ***For more information, see the Company's Insider Trading Policy.***

In addition to these general principals governing insider trading, special rules apply to trading in the Company's securities by certain officers and directors of the Company. These rules are complex, and the Legal Department should be consulted regarding their scope and application.

7.2 Speculative Transactions

It is improper and/or inappropriate for employees to engage in short-term or speculative transactions involving the securities of the Company. Therefore, it is the Company's policy that members of the Board of Directors, officers and employees should not engage in any of the following activities with respect to securities of the Company:

- Trading in the Company's securities on a short-term basis. Any securities of the Company purchased in the open market must be held for a minimum of six months, and ideally, longer. This rule does not apply to the purchase of securities upon the exercise of options that were

granted by the Company.

- Purchases of the Company's securities, including the exercise of options, on margin.
- Short sales of the Company's securities.
- Buying or selling puts, calls, straddles, collars or other similar risk reduction devices with respect to the Company's securities.
- Transactions in publicly-traded options relating to the Company's securities (i.e., options that are not granted by the Company).

8.0 COMMUNICATIONS OUTSIDE OF THE COMPANY

8.1 Communications Regarding Confidential, Proprietary, Privileged, and Secret Information (CPPSI)

Employees should not discuss or disseminate CPPSI (as defined in Section 2.4 above). This prohibition applies to discussions with employees' family members, friends, acquaintances, and other parties even if they have no financial interest in the Company's business.

From time to time, employees may receive calls regarding the Company from securities analysts or the news media. In such situations, the proper response is to inform analysts that questions on behalf of the Company should be directed to the Company's Investor Relations representatives. Similarly, inquiries from the press for comment on behalf of the Company should be directed to the Corporate Communications Department. In the event that employees find that CPPSI has been disclosed in any public forum, they should promptly notify the Investor Relations, Corporate Communications, and/or Legal Department as appropriate. ***See the Contact List at the end of the Code.***

8.2 Communications with Attorneys

Information communicated to Company attorneys or outside counsel retained by the Company generally is protected by the attorney-client privilege. This privilege protects from disclosure to others (including adverse parties in litigation) confidential communications between Company employees and the Company's attorneys made for the purpose of obtaining legal advice on Company business matters. The privilege belongs to the Company, not to employees. Employees should keep such communications confidential and refrain from sharing them with others, including fellow employees or managers, unless authorized or directed by the respective attorney or the Legal Department. Because the privilege belongs to the Company, the Company's attorneys may share with the Company's management any information provided by employees to Company attorneys.

8.3 Blogging and Social Media Communications

Employees may not, on behalf of the Company, publish messages on blogs or engage in social media communications unless approval to do such is granted by the Corporate Communications Department in consultation with the Legal Department. When social networking on behalf of the Company, those authorized employees must post the Company's name, their own name, and their position or title with the Company. For more information, please refer to the ***Veritiv Social Media Usage Policy*** and the ***Veritiv Social Media Guide***.

9.0 SERVICE OF PROCESS AND INSPECTIONS

9.1 Legal Service of Process

Any legal documents served on the Company must be handled in a timely and proper manner. Employees must observe the following guidelines regarding the service of legal documents:

- If someone tries to serve a legal document on the Company, the employee approached should direct them to contact the Legal Department.
- Legal documents, such as service of legal process, left by process servers on Company counters, office lobbies or entrance areas should be promptly forwarded to the Legal Department.
- Answers to any other questions regarding the service of legal documents can be obtained by contacting the Legal Department.

Consistent with the Company's policies regarding the protection of CPPSI, employees are prohibited from providing internal documents or customer files that may contain CPPSI to any outside party simply upon request by the outside party. Outside parties making such request should be advised that Veritiv will respond only to an appropriate service of an appropriate legal document to the Legal Department.

Except as otherwise required by law, the Company does not facilitate the service or acceptance of legal documents directed against individual employees such as service related to personal domestic issues on Company premises. Employees presented with such personal service of legal documents should contact the Legal Department.

9.2 Governmental Searches and Inspections of Company Facilities

If a government agent requests access to Veritiv's premises for inspection, access should not be voluntarily granted (i.e., consent should not be given) unless approval is granted by the Legal Department and the inspection is conducted under the Legal Department's supervision. Notwithstanding the foregoing, employees are directed to fully cooperate with law enforcement agencies that demand or otherwise require a search of the Company's premises or property without the Company's consent. Managers should contact a member of the Legal Department immediately for assistance should any law enforcement agent or other person request official access to the Company's premises or property.

10.0 SOLICITATION, DISPLAYS AND ACCESS TO COMPANY PROPERTY

Veritiv is committed to maintaining a work environment that avoids disruption and promotes the Company's mission and purpose. The Company has established rules, applicable to all employees, to govern solicitation and distribution of literature and the posting of certain information during work time or in work areas. Additionally, the Company has a strict non-solicitation policy as well as a strict protocol regarding the entry of non-employees onto Company premises or facilities. *For more information, see the Company's Non-Solicitation and Distribution Policy.*

11.0 SAFEGUARDING ASSETS

11.1 Use of Company Resources and the Internet

Safeguarding Company and customer assets is the responsibility of all employees. Employees should look for opportunities to improve performance while reducing costs. Except as set forth below, the use of Company time, materials, assets or facilities for purposes not directly related to Company business, or the removing, borrowing, or retaining possession of Company property, including laptop computers, tablets, computer storage devices or media, and smart phones or cell phones, without permission, is absolutely prohibited. Additionally, intentionally using a Company credit card to make personal purchases, even if the employee later repays the Company, is strictly prohibited.

Employees may not use the Company's or any customer's or supplier's money, materials, supplies or other resources, including computers, to advance their outside business interests. Personal calls from office telephones should be kept to a minimum. Use of Company computers, including the Internet and email, for personal matters should be kept to a minimum and generally confined to non-working time such as lunch and breaks.

Internet, intranet and e-mail activities are to be conducted for legitimate business purposes and, subject to the immediately preceding paragraph regarding personal use, other lawful purposes. The Company owns and has all rights to monitor, inspect, disclose and expunge all electronic files and records on Company systems, including all e-mail messages generated using Company facilities, and employees should have no expectation of ownership, use, or rights of privacy with respect to such files, messages and records. Employee use of all Company computing resources, including personal computers, networked services and Internet, intranet and e-mail access (including Web surfing and Web site creation activities) must at all times comply with all Company policies and all applicable laws, including those relating to misappropriation of CPPSI, privacy, sexual and other forms of harassment, and unfair competition or trade practices. Employees must never act in a way that would adversely impact their own job performance, the performance of other Veritiv employees, that brings liability, loss of credibility, or adversely impact Veritiv customers, suppliers, or others who work on Veritiv's behalf.

11.2 Communications Systems and Network Security

Company-owned hardware, software, communications equipment and network systems are provided to employees to conduct the Company's business. Employees are responsible for protecting Company equipment and systems from unauthorized access and/or usage. In addition, employees are prohibited from tampering with or destroying Company systems or equipment.

12.0 POLITICAL AND COMMUNITY ACTIVITIES

The Company encourages employees to become actively involved in their communities. While employees are encouraged to participate in community affairs, they must make it clear that their views and actions are their own, and not those of the Company. In any event, employees should ensure that their outside activities do not interfere with their job performance. Employees who wish to use Company time or property to support civic or charitable efforts must first obtain the approval of his or her manager and the Legal Department.

Corporations are not permitted to make political contributions in connection with any election involving any federal office. There are similar laws in many states and foreign countries. The Company encourages

employees to participate in the political process on their own time, as long as they take care not to imply that they are acting on behalf of the Company. Employees' personal contributions to federal, state or local political campaigns must not be made with, or reimbursed by, Company funds. Individual participation must be completely voluntary, must occur during non-working hours, and may not involve the use of Company funds, personnel time, equipment, supplies or facilities.

Only the General Counsel may authorize an employee to lobby or advocate legislation on behalf of the Company.

No employee is permitted to pressure another employee to express a political view that is contrary to a personal view, or to contribute to a political action committee, political party or candidate, or charitable organization. Employees are also prohibited from posting any unauthorized political or non-Company collateral on Company premises.

For the purposes of this section 12.0, political" activity does not mean "union" activity or other protected organizational activity.

13.0 DATA PRIVACY

All employees are required to comply with laws and regulations governing the collection, use and distribution of personally identifiable data relating to suppliers, customers, employees or others. Employees are required to take reasonable and necessary steps to protect against unlawful access to and disclosure of personally identifiable data and to maintain the highest practicable level of accuracy and integrity of this data.

On occasion, outside parties request from the Company the disclosure of information about a former or present employee. As a general rule, the Company prohibits the sharing of such information with parties outside the Company. In responding to such requests, Company employees are required to observe the Company's employment verification process. No other information about former or current employees may be shared with outside parties, unless directed to do so by the Legal Department.

14.0 OFF-DUTY MISCONDUCT; WORKPLACE VIOLENCE

Employees who engage in any acts of off-duty misconduct may potentially pose a threat to the safety of employees or others, or negatively impact the business image or other assets of the Company.

Accordingly, the Company reserves the right to take disciplinary action, up to and including termination of employment, against employees who engage in behavior outside the workplace that is inconsistent with the Code.

Employees are prohibited from partaking in any type of violence on the Company premises, during working hours or while performing the employee's job, whether on or off premises. This includes, among other things, explicit or implied threats of physical violence (verbal or written), acting in a threatening or aggressive manner, engaging in physical attacks, or fighting, defacing, threatening to deface, damaging,

destroying or stealing Company property or another person's property, or engaging in any other activity that may cause harm to an individual or impact the security of one's personal property.

For more information, see the Company's Workplace Violence Prevention Policy and the Veritiv Preventing Workplace Violence Resource Guide available on the Veritiv intranet.

15.0 REPORTING VIOLATIONS OF THE CODE, OTHER COMPANY POLICIES AND LAW

15.1 How and When to Report Violations

Employees who become aware of illegal activities or unethical conduct at Veritiv - including any violations of Company policy or this Code - have a duty and are required to report. Reports can be directed to the reporting employee's direct-line management, the Human Resources Department, and/or the Legal Department. The HelpLine is an alternative designed to supplement existing reporting channels - not replace them. Employees may file reports by calling the HelpLine (888- 312-2693 in U.S. and Canada; in Mexico 800-462-4240 and then dial 877-556-5341) or emailing http://veritivhelpline.com. Calls or emails to the HelpLine provide the opportunity to identify yourself or to remain anonymous.

The HelpLine may also be used by contractors, vendors and the general public to raise concerns related to potential violations of Company policies or legal compliance.

Ideally, employees should raise concerns before problems develop. By stepping forward and raising ethical concerns, employees can fulfill one of their responsibilities as an employee. They will also be doing the right thing.

Please note that failure to report violations of law may lead to disciplinary action.

15.2 No Chain of Command Required

Employees who report ethical concerns do not have to follow any particular chain of command or sequence. However, managers who receive such reports are generally required to forward them to the Legal Department or, in the case of reports coming from outside the United States, to the senior HR or Legal representative in their region.

15.3 Accounting and Auditing Concerns

All complaints or concerns about accounting, internal accounting controls or auditing matters - regardless of their source or substance - should go *directly* to Internal Audit, the Legal Department or the HelpLine.

15.4 No Retribution or Retaliation

Reporting unethical behavior is vitally important to Veritiv's business, and the Company takes it very seriously. Employees who make such reports in good faith can do so without fear of retribution, retaliation or negative effects on their jobs. Veritiv does not tolerate retaliation — this is the Company's promise to its employees in return for making such reports. Furthermore, anyone who discourages or prevents a fellow employee from making a good-faith report is subject to disciplinary action. Employees should report any attempts to (i) discourage or prevent them from reporting unethical or illegal conduct or (ii) retaliate against or discipline them for making such reports. If you work with someone who has raised a concern or provided information in an investigation, you should continue to treat that person with respect and dignity.

15.5 Advice and Counseling

If an employee needs help or advice regarding ethical business practices, he or she may start by discussing the issues with the supervisor who is most familiar with such employee's daily responsibilities. If an employee is not comfortable going to his or her supervisor for advice, he or she should speak with others, including (i) another manager at their location, (ii) HR – especially with regard to workplace issues, (iii) functional managers, such as from EHS and, Finance, or the Legal Department, and (iv) the HelpLine.

The Legal Department, including the Chief Compliance Officer, is always available to answer any questions about this Code and Company compliance policies or to discuss any concerns employees may have about any of the topics covered in this Code.

15.6 Local Laws

The availability and terms of use of the HelpLine may be limited by local laws. For example, in some countries, callers cannot be anonymous.

15.7 False Accusations

Employees who report a concern do not have to be right about it, but they should honestly believe that such concern is legitimate. To knowingly make a false accusation - or to be uncooperative in an ethical investigation - is a violation of our core values and of this Code.

RESOURCE and CONTACT LIST

Chief Compliance Officer	(770) 391-8232
Chief Security Officer	(770) 391-8342
Corporate Communications	(770) 391-8244
General Counsel	(770) 391-8316
HelpLine	U.S. and Canada: (888) 312-2693 Mexico: (800) 462-4240 and then dial (877) 556-5341 http://veritivhelpline.com
Human Resources Department	(770) 391-8317
Insurance and Risk Management	(770) 391-8242
Internal Audit	(770) 391-8292
Investor Relations	(844) 845-2136 investor@veritivcorp.com
Legal Department	(770) 391-8282