VECTRUS

TRUE TO YOUR MISSION

CODE OF CONDUCT

Version 01
April 2017

VECTRUS.COM

CORE VALUES

INTEGRITY

We act ethically and honestly
We communicate with honesty and courage
We keep our promises
We are trustworthy and consistent in what we say and do

RESPECT

We treat others fairly and courteously
We work as a team and help each other
We sustain a culture of diversity and inclusion
We value different ideas, opinions, and experiences

RESPONSIBILITY

We take ownership of our words and actions
We commit to quality in everything we do
We provide a safe and secure workplace
We care for our communities and the environment

MISSION

Deliver large-scale IT, logistics, and infrastructure services
TO ENABLE CUSTOMER SUCCESS

VISION

Be the customers' first choice and
MOST TRUSTED PARTNER

VALUE PROPOSITION

Cost-effective solutions, performance,
and operational excellence that
EARN THE CONTRACT EVERY DAY

THE VECTRUS DIFFERENCE

OPERATIONAL EXCELLENCE – Teams are certified and processes are compliant
COST LEADERSHIP – High value that earns the contract every day
HONORABLE VALUES – Serve with integrity, steadfast respect, 100% responsibility—always true to our word
CUSTOMER FOCUS – Understand what the customer really wants; hear the voice of the customer
PROGRAM PERFORMANCE – Responsive to the highest standards; engineered to win

VECTRUS
TRUE TO YOUR MISSION

CEO MESSAGE

VECTRUS TEAMMATES:

Welcome to Vectrus. I am proud to present you with this updated Code of Conduct.

As we strive to be our customers' first choice of service provider, we must always act in a manner that models the highest ethical standards and behaviors. Our customers expect this and we should expect nothing less from ourselves. This Code of Conduct is the framework around which we provide exceptional service in all of our work locations.

I expect each Vectrus employee to be familiar with, and abide by, this Code. It is grounded in our core values of Integrity, Respect, and Responsibility, and sets the company's standards of ethical business conduct. By conducting our business in line with these core values, employees, subcontractors, customers, suppliers, and all parties with whom we interact will experience our commitment to ethical conduct.

I am counting on each of you to lead by example. Let this Code guide your decision-making and your interactions with the people around you.

Charles L. Prow
President and Chief Executive Officer

TABLE OF CONTENTS

OUR RESPONSIBILITIES TO DO THE RIGHT THING

Our values of Integrity, Respect, and Responsibility are the foundation for the way we do business, and our success depends upon our unwavering commitment to conducting business ethically and in compliance with all applicable laws and regulations. As part of this commitment, we are all expected to comply with the words and spirit of this Code of Conduct ("Code").

SCOPE AND APPLICATION OF THIS CODE

This Code, and the standards of business conduct and ethics incorporated in the Code, apply to all employees, officers, and directors of Vectrus. Certain business partners and third parties, such as suppliers, agents, representatives, contractors, subcontractors, and consultants, serve as an extension of Vectrus and, as such, are expected to conduct themselves according to our values and standard of ethics when working on behalf of Vectrus.

Any waivers to this code may be granted only by the Board of Directors and will be publicly disclosed as required by law or regulation.

EMPLOYEE RESPONSIBILITIES

Each of us must take personal responsibility for acting according to our company values and this Code, even when this means making difficult choices. We must be committed to living our values and using our Code as a guide for interactions with our stakeholders, including fellow employees, customers, business partners, shareholders, suppliers, third parties, government agencies, and communities. Accordingly, we have the responsibility to:

- Live our company values and abide by the Code, company policies, and the laws and regulations that pertain to an individual's particular job responsibilities.
- Report concerns about possible violations of the Code, company policy, or laws and regulations.
- Complete all required employee training in a timely manner and keep up to date on current standards and expectations.

VIOLATIONS OF EMPLOYEE RESPONSIBILITIES

Violations of the Code, company policies, or laws and regulations will not be tolerated and may result in disciplinary action up to and including termination, legal proceedings and penalties including, in some circumstances, civil or criminal prosecution for both the individual involved and Vectrus.

SUPERVISOR AND MANAGER RESPONSIBILITIES

Leaders, supervisors, and managers have the following additional responsibilities:

- Lead by example and model the highest standards of ethical business conduct and our company values.
- Take the time to ensure your employees know how to use the Code and how to seek additional help.
- Help create a work environment that focuses on building relationships, recognizes effort, and values mutual respect and open communication.
- Be proactive. Look for opportunities to discuss and address ethics and challenging situations with others.
- Create an environment where everyone feels comfortable asking questions and reporting known or potential violations of the Code, policies, or the law.
- Strictly avoid acts of retaliation or behavior that may be perceived by others as retaliation against those who report concerns.
- Respond in a timely and effective manner to concerns that are brought to your attention, but do not feel you must give an immediate response. Reflect, seek advice, and respond later, if needed.

- Never ask or pressure anyone to do something that you would be prohibited from doing yourself.
- Hold employees accountable for completing all training requirements.

COMPLIANCE WITH POLICIES, LAWS, AND REGULATIONS

As a Vectrus employee, you are expected to know and understand the laws, regulations, and company policies that apply to your duties. Regardless of your nationality or country location, you are responsible for complying with all relevant laws and regulations that apply to your work. You must be vigilant in compliance and alert to changes in the law or new requirements that may affect your responsibilities.

Working globally can raise additional ethics and compliance issues because local business and cultural practices may vary. While we respect the norms of our customers and colleagues throughout the world, we must comply with applicable laws and regulations. If you have questions, or if a conflict appears to exist between requirements, stop what you are doing and seek guidance from your supervisor or others listed in this Code.

MAKING ETHICAL DECISIONS

We all take pride in our work and in the choices we make on behalf of Vectrus. These choices may be more difficult to make when we encounter ethical challenges.

When faced with a difficult ethical decision, ask yourself the following questions to determine whether the action you are considering is appropriate:

- Am I adhering to the letter and spirit of our company's policies and to all applicable laws and regulations?
- Is my action consistent with company values and the principles set forth in our Code?
- Would I be acting in the best interests of Vectrus, my coworkers, and our customers?
- What would my family, friends, or neighbors think of my action?

- Would I want my action reported on the front page of a newspaper or on the Internet?

If you are unsure as to what action is appropriate, seek guidance by speaking with your supervisor or with any of the other resources listed in this Code.

ASKING QUESTIONS AND RAISING CONCERNS

OUR STANDARD: If you observe or suspect any illegal or unethical behavior, you are expected to raise the issue to your management or to one of the other resources listed below.

In most cases, you should first contact your supervisor to raise your concerns. However, if you are uncomfortable talking to your supervisor, contact Human Resources, an Ombudsperson, Legal, a compliance representative, or a member of the Ethics and Compliance Review Board (ECRB). You also have the option to report concerns using the EthicsPoint Helpline by telephone or through the Internet.

EthicsPoint Helpline and Complaint Resolution Process

The recommended sequence of steps for resolving employee issues is shown below. This chain of command approach will greatly improve the response time to address your concerns. If you do not feel comfortable with a particular step, skip to the next step.

STEP 1 Contact Your Supervisor or Supervisor's Boss

STEP 2 Contact Your Local HR, Site, Country, or Program Manager

STEP 3 Contact Vectrus Ombudsperson*
systems.ombudsperson@vectrus.com
800.521.3894 or 719.591.3539

STEP 4 Contact EthicsPoint Website*
www.vectrus.ethicspoint.com
866.294.8691 or 503.748.0662

Collect Calls Accepted. **Your complaint can remain anonymous through use of this step.*

Any employee who has a concern or complaint regarding accounting, internal accounting controls, or auditing matters may also report the matter to the Vectrus Head of Internal Audit or the Vectrus

Audit Committee on a confidential or anonymous basis by mail c/o the Vectrus Corporate Secretary, 655 Space Center Drive, Colorado Springs, CO 80915.

Vectrus is committed to enforcing the protections of whistleblowers mandated under the Defend Trade Secrets Act. More information on the Vectrus Defend Trade Secrets Act policy may be found on the Vectrus intranet, by contacting an Ombudsperson, and at https://vectrus.com/dtsa-whistleblower-protections.

In addition, employees may use the Department of Defense Inspector General (DOD IG) Hotline at www.dodig.mil/hotline/hotlinecomplaint.html to report issues related to fraud, waste, abuse, and mismanagement for programs and personnel under the purview of the U.S. Department of Defense.

EXPECTATIONS WHEN USING COMPLAINT RESOLUTION RESOURCES

OUR STANDARD: The EthicsPoint Helpline and website are always available, and all reports of violations will be investigated thoroughly and confidentially.

The EthicsPoint Helpline is available 24 hours a day, seven days a week. This independent third-party provider facilitates the documentation of your concerns and forwards them to the appropriate compliance contact within Vectrus to address.

When making a report, you are encouraged to identify yourself. Doing so facilitates communication and helps Vectrus resolve the situation. However, in the U.S. and elsewhere as allowed by local law, you may make a report anonymously.

If you choose to report anonymously, it is important that you check back with EthicsPoint Helpline, as we may have posted additional questions to help us with our investigation, or we may have provided feedback to you on your concern.

All communications are facilitated by the third-party provider. Access to reported issues is restricted, secure, and confidential in a manner consistent with conducting a thorough investigation and meeting any legal requirements. All issues are investigated thoroughly, and, if appropriate, corrective actions are implemented.

ZERO TOLERANCE OF RETALIATION

OUR STANDARD: There is zero tolerance of retaliation for those employees who, in good faith, report possible ethics or compliance violations.

You can report suspected ethics violations in confidence and without fear of retaliation. Vectrus will not tolerate any retaliation against an employee who, in good faith, asks questions; reports possible violations of the Code, policy, or law; or participates in an investigation.

Reporting "in good faith" means making a genuine attempt to provide honest, complete, and accurate information, even if it later proves to be unsubstantiated or mistaken. Retaliation is a violation of our Code, and knowledge or suspicion of retaliation should be reported immediately.

Vectrus is prohibited by law from discharging, demoting, or otherwise discriminating against employees as a reprisal (collectively referred to as retaliation) for their disclosing of information, either to internal management or to various government agency officials, involving potential evidence of substantial fraud, waste, mismanagement, abuse of authority, threats to homeland security, specific danger to public health or safety, or violation of law related to the performance of U.S. Government contracts.

Any Vectrus employee who believes that he/she has been retaliated against for making a disclosure is encouraged to report the matter to any Human Resource or Legal representative, compliance professional, Ombudsperson, ECRB member, or EthicsPoint Helpline. You may also file a complaint with the DOD IG or the IG of the applicable governmental agency.

COOPERATING WITH INQUIRIES AND INVESTIGATIONS

OUR STANDARD: Cooperate with all internal and external inquiries and investigations.

You are expected to cooperate fully with internal and external audits, investigations, and inquiries that are conducted by the company. In addition, withholding information or knowingly giving false or misleading information is a serious violation of our duties as employees.

In the course of business, you may receive inquiries or requests for information from government officials. Although we are expected to cooperate fully, if you learn of a potential government investigation or inquiry, immediately notify your supervisor and the Legal Department, if possible, prior to taking or promising any action.

With respect to all audits, investigations, and inquiries, you must NOT:

- Destroy, alter, or conceal any document in anticipation of or in response to a request for these documents.
- Provide or attempt to influence others to provide incomplete, false, or misleading statements to a company or government investigator.
- Conduct an investigation yourself; appropriate resources will be assigned to conduct the investigation.

OUR RESPONSIBILITIES TO ONE ANOTHER

We are committed to providing a professional, respectful, and safe work environment. We owe it to each other to be honest and respectful. We should treat others as we would want to be treated.

DIVERSITY AND NON-DISCRIMINATION

OUR STANDARD: Maintain an inclusive and diverse work environment free from discrimination and harassment.

We bring together employees with a wide variety of backgrounds, skills, and cultures. We value different ideas, opinions, and experiences and are committed to sustaining a culture of inclusion and diversity. Combining such a wealth of talent and resources creates the diverse and dynamic teams that consistently drive outstanding results.

We do not tolerate unlawful discrimination of any kind. We provide equal employment opportunities for all regardless of race, color, religion, gender, national origin, age, sexual orientation, physical or mental disability, military/veteran status, marital status, gender identity, ethnic background, or any other legally protected classification.

We do not tolerate harassment of any kind. Verbal or physical conduct that harasses another, disrupts another's work performance, or creates an intimidating, offensive, abusive, or hostile work environment will not be tolerated. Harassing conduct can include inappropriate gestures, remarks, or touching, or displaying sexually explicit or offensive pictures. Promises of promotion or special treatment in return for sexual favors also constitute harassment.

Make sure you:

- Treat others respectfully and professionally, and promote diversity in the workplace.
- Avoid making comments or jokes, or sending or posting materials that others might consider offensive.
- Avoid discrimination against others on the basis of any characteristic protected by law.

- Review your own decisions to ensure that you are using objective and quantifiable standards and business considerations to drive your actions.
- Report all incidents of discrimination, harassment, and intimidation that you observe.

SAFE AND HEALTHY WORKPLACE

OUR STANDARD: Maintain a safe, healthy, and secure work environment.

Vectrus is committed to providing a safe, healthy, and secure workplace for colleagues and visitors to our facilities and to operating in an environmentally sound manner. Vectrus requires that all employees practice safe work habits and follow all applicable safety, security, and health rules and practices.

Make sure you:

- Review and follow the safety, security, and health rules and practices that apply to your job and your facility.
- Complete required training and follow the additional security procedures required for secure areas.
- Immediately report any practices or situation, regardless of severity, that could pose a threat to the environment or to the safety or health of anyone.

Drugs and Alcohol

To maintain a safe workplace, it is essential that we are able to think clearly and react quickly. Any involvement with illegal drugs, including their use, possession, distribution, purchase, sale, offer for sale, or manufacture, while on Vectrus premises, on company time, or when conducting or travelling on company business is prohibited. The abusive use of controlled substances, including prescription drugs or alcohol, is also prohibited. The only exception to this rule is when alcohol is consumed responsibly and in observation of applicable laws at business dinners or in accordance with local management direction at an authorized company event.

Workplace Violence

Violence of any kind has no place at Vectrus. We will not tolerate any acts or threats of physical violence against coworkers, visitors

or anyone on Vectrus property, or by any representatives of Vectrus during company travel or company-sponsored events. Prohibited activities include:

- Threatening remarks or behavior, obscene phone calls, or stalking.
- Assaults or causing physical injury to another.
- Intimidation or acting aggressively in a manner that causes someone else to fear injury.
- Intentionally damaging someone else's property.
- Bringing prohibited weapons and other items, such as explosives or fireworks into company facilities or to company-sponsored events.

Every threat of violence is serious, and you are expected to immediately report any observations of violence to your supervisor, any member of management, Human Resources, or Security.

ENVIRONMENTAL STEWARDSHIP

OUR STANDARD: Protect the environment and conserve natural resources.

We conduct our business in a way that protects the environment for future generations. We work with our business partners and suppliers to strengthen environmental stewardship and responsibility, while respecting the communities where we do business.

We are committed to meeting or exceeding applicable environmental laws and regulations, and company policies, and to continuously improving our environmental performance through resource conservation, waste minimization, water and energy efficiency, and the effective use of raw materials.

Make sure you:

- Comply with all applicable environmental laws, regulations, and company policies.
- Report any incident or conditions that might result in an environmental violation, pose a hazard, or waste natural resources.
- Do your part to reduce water and energy use.

- Identify opportunities for improving our conservation and recycling efforts.

HUMAN RIGHTS

OUR STANDARD: Recognize and adhere to internationally recognized human rights provisions.

We support human rights by complying with internationally recognized provisions in all locations where we operate, regardless of local business customs, and are committed to providing safe and secure conditions for those working on our company's behalf.

We will not knowingly work with commercial business partners that employ children or forced labor, including prison or bonded labor. We will not tolerate physical punishment or abuse. We will not engage in human trafficking-related activities to include: misleading or fraudulent recruiting practices, charging our employees recruiting fees, confiscating or destroying employee identification documents, or supporting prostitution. It is a violation of company policy and Federal Law for employees to, directly or indirectly, purchase commercial sex acts for themselves, for the benefit of employees or third parties, or while conducting company business.

Make sure you:

- Immediately report any suspected potential human rights-related violations.
- Strictly prohibit use of child or forced labor, including prison or bonded labor.
- Commit to obeying the associated laws and regulations, and where these laws vary or conflict, follow the highest standards.

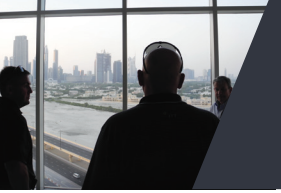
PRIVACY OF EMPLOYEE INFORMATION

OUR STANDARD: Handle employee information responsibly.

For those of us who have access to personal information related to our colleagues and others, we have an obligation to protect this information and exercise caution prior to disclosing it to others. This includes, but is not limited to, medical, payroll, and personally identifiable information. We may only provide employee information to other employees and third parties where permitted by law.

Make sure you:

- If you have access to employee information, learn which types of information are given heightened protection by the law and company policy (such as government-issued identification, bank account numbers, and medical records) and protect them through appropriate means (such as encryption or other types of limited access).
- Protect the confidentiality of personal information of current and former colleagues, as well as job applicants, business partners, and customers.
- Don't access, discuss, or share confidential information unless there is a legitimate business reason to do so.
- Immediately report any loss or inadvertent disclosure of confidential employee information.
- Ensure recipients of employee information will safeguard the information.



FAIR AND OPEN COMPETITION

OUR STANDARD: Recognize and avoid anti-competitive behaviors and activities.

We believe in fair and open markets and never engage in improper practices that may limit competition. We compete vigorously to be an industry leader, and we do so by maintaining high standards of fairness and honesty when engaged in marketing, promotional, and advertising activities. We look to gain competitive advantage through superior performance, price, and quality and not through unethical or illegal business practices.

We do not enter into agreements with competitors to engage in any anti-competitive behavior, including setting prices or dividing up customers, suppliers, or markets.

Anti-trust laws are complex, and compliance requirements can vary depending on the circumstance, but, in general, the following activities are "red flags" and should be avoided and reported to your supervisor or the Legal Department:

Collusion

When two or more parties secretly communicate or agree on how they will compete. This could include agreements or exchanges of information on pricing, terms, wages, or allocations of markets.

Bid-Rigging

When two or more parties manipulate bidding so that fair competition is limited. This may include comparing bids, agreeing to refrain from bidding, or knowingly submitting noncompetitive bids.

Tying

When a company with market power forces customers to take products or services that they do not want or need.

Predatory Pricing

When a company with market power sells a product or service below cost so as to eliminate or harm a competitor, intending

to recover the loss of revenue later by raising prices after the competitor has been eliminated or harmed.

Make sure you:

- Never share the company's sensitive information with a competitor of the company.
- Never share sensitive information of business partners or other third parties with others without their permission.
- Never take advantage of anyone through manipulation, abuse of privileged information, misrepresentation of facts, or any other intentionally unethical or illegal action.
- Never engage in conversations with potential competitors about competitive sensitive information.
- Never use or disseminate non-public information about potential competitors from new hires or candidates for employment.
- Never have conversations with potential competitors that could be perceived as limiting competition.

ZERO TOLERANCE FOR CORRUPTION AND BRIBERY

OUR STANDARD: Vectrus has zero tolerance for acts of bribery and corruption. Do not offer or provide bribes to influence action or accept kickbacks in connection with company business.

Vectrus is committed to conducting business ethically, with integrity, and in compliance with applicable laws and regulations prohibiting bribery, kickbacks, and other forms of corruption in our operations worldwide. Because of the complexity of anti-corruption and bribery laws, it is important that employees are aware of company policies and ask questions if they have any doubts about the proper course of action. Bribery and kickbacks are never permitted at Vectrus, regardless of whether we are dealing with a government or commercial customer.

A **BRIBE** is the payment of anything of value, such as cash, gifts, services, contributions, internships, or vacations made for the purpose of improperly obtaining or retaining business.

A **KICKBACK** is the return of a sum already paid or due to be paid, as a part of a legal contract, as a reward for making or fostering business arrangements.

The U.S. Foreign Corrupt Practices Act (FCPA), the United Kingdom Bribery Act, and the laws of most countries in which we operate all

prohibit bribing government officials. For purposes of these laws, the term "government official" is defined broadly and includes civil servants, officials of state-owned or controlled commercial enterprises, representatives of public international organizations, office seekers, political parties, family members, and political party officials. Many countries also have laws that prohibit bribes paid to private individuals.

It is especially important that employees carefully monitor third parties acting on the company's behalf. We must always be sure to perform due diligence and know our business partners and all those through whom we conduct our business. Our third parties must understand that they are required to operate in strict compliance with our standards and to maintain accurate and complete books and records.

Facilitation payments are not allowed by company policy and are a violation of some international norms and national laws, such as the U.K. Bribery Act. You must obtain approval from the Legal Department before making a facilitating payment no matter how small the amount. If you are solicited for a facilitation or expediting payment, contact the Legal Department immediately.

FACILITATION OR EXPEDITING PAYMENTS

Sometimes known as "grease payments," facilitation or expediting payments are modest amounts of money paid as an unofficial fee to low-level government employees to expedite or initiate the performance of routine and expected government services to which Vectrus is entitled.

A facilitating payment can be made if an individual's health or safety is being imminently threatened and there is no practical opportunity to secure advance authorization from the Legal Department. The payment must be reported to the Legal Department as soon as possible.

Examples of facilitating payments are offering small fees to low-level foreign government officials to expedite processing of a permit, license, or other official document, processing visas or work orders, or providing phone, water, and power service.

Make sure you:

- Never directly or indirectly offer, provide, or authorize money or any item of value to improperly obtain or retain business or to improperly influence a governmental action.

- Never make payments that are intended to improperly influence a government official.
- Never directly or indirectly request, agree to receive, or accept kickbacks, payoffs, or other personal payments in connection with company business.
- Notify the Legal Department of third parties or agents who are thought to be valuable primarily for their personal ties rather than for the services they are to perform or who request compensation out of proportion to their services.

Anti-Money Laundering

Vectrus does not condone, facilitate, or support money laundering. Involvement in such activities undermines our integrity, damages our reputation, and can expose Vectrus and individuals to severe sanctions.

MONEY LAUNDERING occurs when companies or individuals attempt to convert, disguise, or hide proceeds of illegal activity by moving illegally obtained funds, or by hiding the source so the funds are made to appear legitimate.

Employees must comply with all applicable money-laundering and anti-terrorism requirements that prohibit:

- Engaging in financial transactions involving property, funds, or monetary instruments that, directly or indirectly, promote or result from criminal activity.
- Receiving, transferring, transporting, retaining, using, structuring, diverting, or hiding the proceeds of any criminal activity, or aiding or abetting another in any such action.
- Engaging or becoming involved in financing, supporting, or otherwise sponsoring, facilitating, or assisting any terrorist person, activity, or organization.

Make sure you:

- Never cooperate with efforts to evade reporting requirements.
- Report suspicious activity, such as payments to offshore banking locations, payments to third parties outside the territory in which the third party operates, and false invoices for sales.

BUSINESS COURTESIES

OUR STANDARD: Do not accept or provide business courtesies if the intent is to improperly influence a business decision.

Conducting business with integrity means never seeking to improperly influence business decisions. For this reason, it is important for each of us to exercise common sense and good judgment when giving or receiving business courtesies. Before giving or receiving a business courtesy you must review the Vectrus policy on business courtesies and use the Business Courtesy Request System as required by policy.

A **BUSINESS COURTESY** is any item of value provided to or received from a third party for the purpose of initiating or furthering a business relationship. Business courtesies include such things as cash, entertainment, meals, gifts, social events, sporting events, travel, lodging, favors, gratuities, discounts, and services.

In general, we may not offer or accept a business courtesy if it:

- Violates any law, regulation, or policy applicable to the giver or recipient.
- May be considered a bribe, payoff, or kickback.
- Violates customary business practices.
- Gives the appearance of impropriety or could give rise to a conflict of interest.

We must always avoid situations where business courtesies could harm the reputation of our company or those of us involved. Please note that we may never attempt to circumvent these rules by using our personal funds or by engaging an agent or representative to pay for any business courtesy that we cannot pay ourselves. The rules outlined in this section also govern the actions of our family members and close friends, as well as those of Vectrus' agents and representatives. If you have concerns related to business courtesies, contact the Legal Department.

Government Officials

U.S. Government Officials

The U.S. Government has strict laws and rules prohibiting its employees or elected representatives from accepting business

courtesies. With the exception of common hospitality and promotional items of nominal intrinsic value, we may not offer or give a business courtesy to a government official without the prior written approval of the Legal Department.

Non-U.S. Government Officials

Most countries prohibit their official employees from accepting business courtesies. With limited exceptions, business courtesies extended to any government officials require prior written approval from the Legal Department.

Make sure you:

- Coordinate with the Legal Department for review and approval prior to providing any business courtesy to any government official no matter the country they represent.
- Are aware of the perceptions that can be drawn from the provision of business courtesies to government employees.
- Exercise caution when dealing with business partners, which could appear to be privately owned but are actually considered government entities.

Commercial Third Parties

Exchanging business courtesies with our commercial third parties must be reasonable, infrequent, for a legitimate business reason, and consistent with normal industry practice and local laws.

Providing or offering business courtesies to commercial third parties that exceed nominal value may require written Legal Department approval. Before giving or receiving a business courtesy from a commercial third party you must review the Vectrus policy on business courtesies and use the Business Courtesy Request System as required by the policy. Exceptions include coffee, soft drinks, light snacks, an inexpensive business-related meal incident to a site visit, recognition awards for program or service achievements, or promotional items.

Make sure you:

- Seek guidance and approval if you are unsure as to whether the business courtesy is appropriate.
- Only provide and accept business courtesies that are justified by the business relationships. Keep in mind that exchanging business courtesies that foster goodwill in business relationships

is generally acceptable, but you should never provide or accept business courtesies that obligate or appear to obligate the recipient.

- Do not offer or accept lavish, extravagant, or unreasonable business courtesies.
- Do not offer travel and lodging without advance approval from your Legal Department.
- Understand and comply with both Vectrus and third-party policies before offering or providing business courtesies.
- Raise a concern whenever you suspect that a colleague, third party, or other agent of the company may be engaged in an attempt to improperly influence a decision of a customer.

Specifically regarding the acceptance of business courtesies:

- Do not request or solicit personal gifts, favors, entertainment, services, or any other type of business courtesy.
- Never accept cash or cash equivalents, such as gift cards, of any value.
- Never accept business courtesies of any kind from a business partner with whom you are involved in contract solicitation or negotiations.
- Refuse business courtesies that seem inconsistent with our business practices and report it to your supervisor.
- Seek advance written approval for any exceptions.

EXPORT/IMPORT CONTROLS

OUR STANDARD: Fully comply with export/import laws and do not trade with sanctioned or embargoed countries or entities.

In the U.S. as well as other countries in which Vectrus operates, governments often have complex and significant restrictions on trade in military and dual-use goods, technology, and services, as

An **EXPORT** occurs when a product, service, or technology is transferred either physically across borders; electronically via the Internet, fax, e-mail, or data-sharing sites; or visually through demonstrations, presentations, and discussions between nationals of different countries. Such exports, if they involve controlled military or dual-use technologies, often require government approval in the form of an export license or other authorization.

well as trade with certain countries. Vectrus complies with all trade restrictions and import and export control laws of the countries in which we operate. We expect all of our business partners, third parties, consultants, and contractors to do the same. Limited exceptions may apply in cases where such laws conflict with U.S. laws (see Boycotts). Export rules may restrict the following:

- Any oral discussion with any non-U.S. person, even someone inside the U.S., which discloses technical information and might be considered an export.
- Using business knowledge outside of the employee's country, such as when providing technical assistance to others.
- Transferring technical data to someone in another country, such as through the Internet, e-mail, conversations, meetings, and network or database access. This restriction applies to sharing information with other company employees, as well as non-employees.
- Transferring technology to non-U.S. persons, whether located inside or outside the U.S.
- Transferring technology from an authorized non-U.S. person to one that is not authorized.
- Transporting, carrying, or sending a controlled defense article or technical data about a defense article outside the U.S.

Trade restrictions also involve prohibitions against dealing with specifically identified sanctioned or embargoed countries or entities acting on their behalf, as well as on transactions involving certain named persons or organizations.

An **IMPORT** occurs when products purchased or obtained from a foreign country or external source are brought into another country. Import transactions are subject to laws and regulations and must go through Customs' formalities for the assessment of necessary duties and taxes.

At times, export control laws in certain regions may conflict. To avoid problems, employees must consult Trade Compliance or the Legal Department as early as possible about local laws on exporting products, information, and technology.

- Comply with all export and import laws, regulations, and requirements and with Vectrus trade-control policies.

- Understand the trade controls related to Vectrus products, technology, and information and the restrictions on transferring those items to entities outside the company.
  - Obtain licenses or other government approvals prior to exporting and importing products and technology controlled by the Government.
  - Report any known or suspected trade-control violation to the Vectrus Trade Compliance Department.
- Report complete, accurate, and detailed information regarding every imported product, including its proper classification, country of origin, and appropriate value.

We may not participate in or promote boycotts that the U.S. does not support, such as the Arab League Boycott of Israel. This means that we may not agree to a contract, document, or verbal request containing language that could be interpreted as an attempt by a person, group, or country to enforce an unsanctioned boycott.

BOYCOTTS occur when a person, group, or country refuses to do business with certain persons, groups, or countries as a means of protest, an expression of disfavor, or a method of coercion.

Make sure you:

- Review all transactional documents, including contracts, letters of credit, shipping or import documents, or bid and proposal materials, for any language that may constitute a boycott request.
- Notify the Trade Compliance Department or Legal Department if requested to join in, support, or furnish information concerning a non-U.S. boycott.

POLITICAL INVOLVEMENT

OUR STANDARD: Do not support political parties on the company's behalf or engage in prohibited lobbying activities.

We believe that our employees benefit from being active in the community through good citizenship. We recognize that our employees have a right to voluntarily participate in the political process, including volunteering in campaigns and making individual political contributions. Vectrus also has a clear and separate responsibility to obey all applicable laws and regulations with

regard to operation of a corporate Political Action Committee and employing registered lobbyists for company business. These separate individual and company activities need not be in conflict provided that employees exercising their rights do so only in their own name and on their own time. Never use the company name, funds, assets, services, or facilities to support any political candidate or party or to engage in any lobbying activity unless specifically permitted by law and authorized in advance by the Communications and Legal Departments.

Make sure you:

- Consult with our Communications and Legal Department professionals BEFORE interacting with government officials in a manner that might be interpreted as a lobbying activity.
- Ensure that your personal political views and activities are not viewed as those of the company.
- Do not use the company's name, resources, or facilities to support your personal political activities.
- Never apply direct or indirect pressure on another employee, customer, or business partner to contribute to, support, or oppose any political candidate or party.
- Avoid the appearance that you are making political or charitable contributions in order to gain favor on behalf of Vectrus.
- Notify management prior to accepting or campaigning for political office.

OUR RESPONSIBILITIES TO OUR BUSINESS PARTNERS

HONEST AND ETHICAL DEALINGS

OUR STANDARD: Maintain a culture of integrity by being honest and ethical in business relationships.

We treat all of our business relationships fairly: the government, our non-government customers, business partners, third parties, suppliers, and contractors. We work to understand and meet their needs, while always remaining true to our own ethical standards. We tell the truth about our services and capabilities, and we do not make promises we know we cannot keep. In short, we treat our business partners as we would like to be treated.

We expect our customers, business partners, and stakeholders to act in a manner that is consistent with our ethical standards, and we must bring suspected unethical or illegal activity on their part to the immediate attention of the Vectrus Legal Department.

Make sure you:

- Talk to your supervisor if you have concerns about any error, omission, undue delay, or defect in quality or customer service.
- Report pressure from colleagues or managers to cut corners on quality or delivery standards.
- Never follow a customer's or third party's request to do something that you regard as unethical or unlawful.
- Respond promptly to customer and business partner requests and questions.
- Promise what you can deliver and deliver on what you promise.

PROCUREMENT INTEGRITY

OUR STANDARD: Understand and comply with the procurement integrity laws and regulations.

Since we conduct business with governments and government-owned entities, we are committed to compliance with many special legal, regulatory and contractual requirements that apply to government contracting. In compliance with the Procurement Integrity Act, we will not disclose or use any unauthorized

confidential contractor bid or proposal information, or source selection information before a contract award. Employees should contact their Contracts or Legal Departments with questions specific to contracting with the government.

BID OR PROPOSAL INFORMATION is typically proprietary information submitted by the bidding entity.

SOURCE SELECTION INFORMATION is any information prepared for use by a federal agency for evaluating bids or proposals to enter into a procurement contract.

Hiring Former Government or Military Personnel

The U.S. Government and other countries have laws and special restrictions that apply to the recruitment and hiring of current and former government employees and military personnel as employees, consultants, or representatives. Restrictions include limitations on the type and timing of employment-related discussions that government employees may have with Vectrus. We must ensure that such employment discussions are approved in advance by company Human Resources and Legal Departments.

Make sure you:

- Avoid seeking or receiving information that the company is not authorized to possess, such as confidential or proprietary data, pricing information of other competitors, and non-public government documents relating to bidding or source selection.
- Seek immediate guidance from the Legal Department if you inadvertently receive unauthorized bid or proposal or source-selection information.
- Comply with government conflict-of-interest restrictions.

ORGANIZATIONAL CONFLICTS OF INTEREST (OCI)

OUR STANDARD: Disclose any potential organizational conflicts of interest.

We are required to recognize and avoid organizational conflicts of interest in connection with direct or indirect contracts with the U.S. Government. An OCI may arise where activities of the company, our employees, partners, or competitors could impair the ability of another to render impartial services to a direct or indirect contract with the government. This could also give an unfair advantage in competing for a contract because of access to information obtained as a result of other contractual relationships with the government.

BUSINESS PARTNER RELATIONS

OUR STANDARD: Business partner relationships must be based on mutual trust and a commitment to act with integrity.

We deal fairly with our suppliers, consultants, and other third parties, and we expect them to act with integrity. We expect business partners to follow terms and the spirit of our Supplier Code of Conduct, as well as any applicable contractual provisions, when working in connection with Vectrus.

Due Diligence

Appropriate due diligence must be performed by Vectrus before engaging any third-party that will be marketing or distributing Vectrus products and services outside the U.S., including enhanced due diligence for third parties that will have contact with U.S. and non-U.S. government customers and other government employees and officials on behalf of Vectrus.

Supplier Diversity

Recognizing the importance and benefits of a diverse supplier base, we will work to identify qualified minority- and woman-owned business enterprises, small business, other recognized disadvantaged businesses, and local business enterprises capable of providing products and services.

Subcontractor Code of Ethics Provisions

For U.S. Government contracts above a specific value, the law requires that we will ensure applicable subcontracts include the provision to have and maintain a code of conduct and an ethics and compliance program that includes training, an internal reporting mechanism, and discipline for code violations.

Product Origin, Quality, and Substitution

Our customers, both government and commercial, have the right to insist on strict compliance with contract requirements. We must only deliver products and services that conform to the contract's specified requirements. We must avoid the substitution of lower-quality, different, or inadequately tested products. We must also ensure that suppliers of raw materials, parts, and components used in our products meet our contract requirements.

CONFLICTS OF INTEREST

OUR STANDARD: Disclose and seek guidance on any issues that may conflict with your responsibilities with the company.

A conflict of interest occurs whenever you have competing interests that may interfere with your ability to make an objective decision in the best interest of Vectrus. Each of us is expected to adhere to the Vectrus Conflicts of Interest Policy, use good judgment, and avoid situations that can lead to even the appearance of a conflict of interest, as it could undermine the trust that our customers, business partners, fellow employees, and the public place in us.

Below are some areas in which potential conflicts of interest may arise:

Personal Relationships

Personal relationships with employees or business partners, such as family members, friendships, and romantic partners, who have influence over one another through the chain of command, in purchasing or contracting decisions, in bidding or proposal-related efforts, or in recruiting or hiring decisions.

Financial Dealings and Investments

Situations where you or a family member has a significant financial ownership interest in a privately or publicly owned enterprise with which Vectrus competes or does business.

Outside Employment

Since outside employment may appear to bias our decisions against the best interest of Vectrus, we may not be employed by, work as a consultant for, or be affiliated with a Vectrus competitor, customer, or supplier. You should always discuss any outside work situations with your supervisor prior to undertaking them.

Make sure you:

- Always make business decisions in the best interest of Vectrus.
- Seek guidance to avoid potential conflicts of interest.
- Disclose potential conflicts immediately by notifying your supervisor or Human Resources in writing.
- Notify your supervisor of any outside employment.

BUSINESS INTELLIGENCE

OUR STANDARD: Obtain competitive information only through proper means.

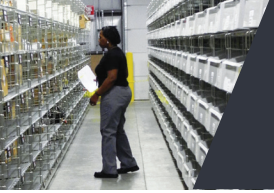
Information about competitors is a valuable asset in today's competitive business environment. When collecting business intelligence, Vectrus employees and others who are working on our behalf must always live up to the highest ethical standards.

We must never engage in fraud, misrepresentation, or deception to obtain information. Nor should we use invasive technology to "spy" on others. We also need to be careful when accepting information from third parties. You should know and trust their sources and be sure that the knowledge they provide is not protected by trade secret laws, or non-disclosure or confidentiality agreements.

When Vectrus employs former employees of competitors, we recognize and respect the obligations of those employees not to use or disclose the confidential information of their former employers.

Make sure you:

- Do not request or receive the confidential information of other companies.
- Never pressure new employees to discuss confidential information from their previous employers.
- Do not disclose suppliers' non-public pricing information.
- Never retain papers or computer records from prior employers in violation of laws or contracts.
- Do not seek information obtained through any behavior that could be construed as "espionage," "spying," or that you would not be willing to disclose fully.
- Do not disclose proprietary information belonging to your prior employer.
- Do not use for any other purpose proprietary information provided under a non-disclosure agreement for a particular purpose.



OUR RESPONSIBILITIES TO OUR SHAREHOLDERS AND THE FINANCIAL MARKETPLACE

ACCURACY OF RECORDS

OUR STANDARD: Maintain current, accurate, and complete business records.

Our shareholders, business partners, customers, government officials, and the public need to be able to rely on the accuracy and completeness of our disclosures and business records. Accurate information is also essential within the company so that we can make good decisions.

RECORDS are any information generated during the course of company business and include not only paper documents, but also tapes, photographs, computer files, and records in any other form.

We are responsible for honesty and transparency in the preparation and maintenance of our business records, including our time cards, expense reports, quality, safety, and procurement records. Employees with a role in financial or operational recording or reporting have a special responsibility in this area, but all of us contribute to the process of recording business results and maintaining records. Each of us is responsible for helping to ensure the information we record is accurate, complete, and maintained in a manner that is consistent with our internal controls.

Charging Costs

All costs allocated to a particular government contract as direct or indirect costs must be reasonable, allocable, and allowable under applicable procurement cost principles and Cost Accounting Standards in accordance with applicable Disclosure Statements. In addition, when we work on government contracts or subcontracts, we must:

- Accurately record the number of hours worked to the appropriate project.
- Charge all labor and material costs to the proper contract and charge indirect costs properly.
- Ensure only costs properly chargeable to a government contract are billed to the government.

Records Retention

We are responsible for the information and records under our control, and we must be familiar with the recordkeeping procedures that apply to our jobs. It is also our responsibility to keep our records organized so that they can be located and retrieved when needed.

Documents should only be destroyed in accordance with our record-retention schedule, and never in response to, or in anticipation of, an investigation, audit, or pending litigation. Contact the Legal Department if there is any doubt about the appropriateness of record destruction.

Legal Holds

A legal hold suspends all document destruction procedures, including deletion of e-mails and computer files, in order to preserve appropriate records under special circumstances, such as litigation or government investigations. Vectrus will determine and identify what types of records are required to be placed under a legal hold. Every employee, agent, and contractor must comply with this policy.

If there is any question as to whether a record pertains to an investigation or legal proceeding, contact the Legal Department prior to disposing of any related records.

Make sure you:

- Submit current, accurate, and complete business records at all times.
- Report your suspicions or observations of others who create inaccurate records.
- Act promptly, in consultation with management, to correct any discrepancies.
- Write truthfully, objectively, and clearly in all your business communications, including e-mails.
- Sign documents, including contracts, only if you have reviewed, are authorized to sign, and believe them to be accurate and truthful.
- Do not hide or disguise the true nature of any transaction.

COMPANY ASSETS

OUR STANDARD: Appropriately use and protect company assets, as well as those of our customers and suppliers.

We are entrusted with company- and government-provided assets and are personally responsible for protecting them against theft, loss, or abuse and for using them appropriately and for business purposes. Property provided by the government customer or other third party must be used and managed according to the terms of the relevant agreement or contract.

COMPANY ASSETS include Vectrus products, funds, facilities, equipment, vehicles, information technology, intellectual property, proprietary and confidential information, as well as our company's reputation.

Information Technology

Information technology is a valued asset and is provided for the business use of our employees. We should use Vectrus information technology, such as Internet, e-mail, computers, and mobile devices, for authorized, business purposes and may not use these resources to view, download, or communicate inappropriate, unprofessional, or illegal content. This includes content that could be considered obscene or offensive, unlicensed software, and copyrighted materials.

Personal use of Vectrus' information technology is discouraged and should be kept to a minimum. Any occasional personal use of our information technology should not adversely affect your productivity or the work environment.

Since the information technology we use when working for Vectrus belongs to our company, you should not have an expectation that e-mails, Internet activity, computer files, and the like are private. Vectrus reserves the right to review all information technology usage and will do so in accordance with the law.

Make sure you:

- Immediately report any suspicions of fraud, theft, or misuse of company assets.
- Do not share passwords or allow other people to use company resources.

- Do not attempt to access any data that you are not authorized to view.
- Do not download, install, or run unauthorized or unlicensed software on company information technology.
- Never copy, install, or use company software for personal purposes.

SENSITIVE INFORMATION

OUR STANDARD: Protect company proprietary, customer confidential and classified information, and intellectual property from unauthorized disclosure.

Proprietary Information

PROPRIETARY INFORMATION

Some common examples of what may be considered company-proprietary information include business plans, contract proposals and bids, company initiatives, pricing, phone lists, and other non-public information.

Company proprietary information is one of our most valuable assets, and each of us must be vigilant in protecting it. This means keeping company-proprietary information secure, limiting access to those who have a need to know, and avoiding discussions in public areas. It is also expected that you will not share the company's proprietary information with anyone outside the company, even after your employment with Vectrus ends.

Make sure you:

- Use and disclose company proprietary information only for legitimate business purposes and when authorized.
- Properly label proprietary information to indicate how it should be handled and distributed.
- Dispose of proprietary information in designated receptacles.
- Know which types of information are given heightened protection by the law and company policy, such as personally identifiable information, government-issued identification numbers, and bank account numbers.

Customer Confidential Information

Our customers place their trust in us, and, in turn, we must protect their confidential information. We may only disclose customer-

confidential information to coworkers who have a legitimate business need to know, and should not disclose it to people outside our company without authorization.

Make sure you:

- Understand and adhere to the laws, regulations, company policy, and agreements on the use, protection, and retention of information from or about customers.
- Immediately report any loss or inadvertent disclosure of customer information.
- Take steps to ensure that customer information is secure when off company premises.
- Never use customer information for personal gain.

Classified Information

In many situations, governments have entrusted special information to us that may be classified or require special handling. We have a continuing obligation to protect classified information. Security regulations that relate to the protection of government-classified information are complex and vary by country and government agency. We are required to properly safeguard and control access to this information in accordance with the security guidelines prescribed by the contract, country, or government agency.

Make sure you:

- Are familiar with applicable security regulations and hold the applicable clearance prior to accessing classified information.
- Immediately report any known or suspected security infraction or violation.
- Only give individuals access to classified information if it has been approved, they possess the necessary clearance level, and if they have a need to know.
- Promptly self-report to your security officer any issue requiring disclosure by the NISPOM and its categories of reportable information, any suspicious contacts, any attempts to compromise protected information, and or any other information required to be reported under applicable agency security program requirements.

INTELLECTUAL PROPERTY

Vectrus retains exclusive ownership of the intellectual property in any idea, process, trademark, invention, or improvement you create while working for the company. Vectrus must protect our intellectual property carefully as a corporate asset.

We must also safeguard the intellectual property entrusted to us by others—particularly customers, suppliers, and business partners—and not infringe upon the intellectual property rights of others.

INTELLECTUAL PROPERTY includes the following types of information:

- Patents, trademarks, and copyrights
- Trade secrets
- Technical data and software developed under or used in support of customer contracts
- Inventions and discoveries
- Methods, know-how, and techniques
- Innovations and designs
- Systems, software, and technology
- Brands

Make sure you:

- Report any suspected theft, misuse, or improper disclosure of the company's intellectual property.

INSIDER TRADING

During the course of our employment at Vectrus, we may come to know material information about our company or business partners before it is disclosed to the public. This information is often called "inside information," and we are prohibited from trading securities or passing information on to others who then trade on the basis of this information.

Make sure you:

- Do not buy or sell securities of our company when you have inside information.
- Do not communicate inside information on Vectrus to other people, including family members or friends.

INSIDE INFORMATION is information that is confidential, material, not yet disclosed to the public, and that a reasonable investor would take into consideration when deciding whether to buy or sell a security. Some examples of information about a company that might be considered "inside information" are:

- A proposed acquisition, merger, or sale
- A significant expansion or cutback of operations
- A significant product development effort
- Pending award of a substantial contract
- Changes in company's senior management or executive structure
- Extraordinary management or business developments
- Sensitive corporate financial information

PUBLIC COMMUNICATIONS

OUR STANDARD: Only authorized persons may speak on behalf of the company.

We are committed to provide accurate and consistent information regarding our operations, products, and services to the public, and we must exhibit objectivity, openness, and honesty in our communications. As a publicly traded company, we are also subject to regulations that govern how we must disclose material financial information. To meet our standards, Vectrus needs a consistent voice when making disclosures or providing information. It is important that only authorized persons speak on behalf of the company.

Make sure you:

- Never speak publicly on issues involving the company without prior authorization from a member of the Corporate Communications team.
- Obtain approval from the Communications team prior to making public speeches or writing articles for professional journals when you are identified as being an employee of the company.
- Obtain approval from the Communications team before distributing any communication intended for a broad employee audience.
- Never give the impression that you are speaking on behalf of the company in any personal communication, including user forums, blogs, chat rooms, and bulletin boards.

SOCIAL MEDIA

OUR STANDARD: Use social media responsibly and in accordance with company values and policies.

If you participate in online forums, blogs, wikis, chat rooms, bulletin boards, or other social networks, never give the impression that you are speaking on behalf of Vectrus unless you are authorized to do so. If you reveal that you are a Vectrus employee, make it clear that your views are yours alone. Despite privacy settings, all social media are inherently public communication channels, so always think carefully before posting content online.

Make sure you:

- Never post company-confidential, export-restricted, or classified information. Never post false information or anything that might defame others or damage our brand or reputation.
- Never post material that is obscene, threatening, or abusive toward a coworker, consultant, contractor, customer, supplier, or competitor.
- If you ever have questions about what is or what is not appropriate, contact a member of the Communications team.

SUMMARY

The Vectrus Code of Conduct articulates for our employees, our customers, and other stakeholders the ethical standard that governs both our business conduct and our relationships with one another.

The Code is intended to help Vectrus employees understand and adhere to these standards in their daily activities, consistent with our core values of Integrity, Respect, and Responsibility, and is not intended to serve as a replacement for the laws, regulations, and internal policies that govern our operations.

CONTACTS

If you have questions or concerns and would like to speak with someone for advice on ethics or compliance matters, contact your local or Corporate Human Resources Department, Legal Department, or Ethics and Compliance Department.

If you prefer to speak with someone outside of your business area, you may contact our third-party helpline provider, EthicsPoint, or the Vectrus Ombudsperson, who is a Vectrus headquarters employee, at systems.ombudsperson@vectrus.com, 800.521.3894 or 719.591.3539.

EthicsPoint Helpline

Phone: **866.294.8691** or **503.748.0662**
Collect calls are accepted.

Web: **www.vectrus.ethicspoint.com**

Any employee who has a concern or complaint regarding accounting, internal accounting controls, or auditing matters may also report the matter to the Vectrus Head of Internal Audit or the Vectrus Audit Committee on a confidential or anonymous basis by mail c/o the Vectrus Corporate Secretary, 655 Space Center Drive, Colorado Springs, CO 80915.

Vectrus is committed to enforcing the protections of whistleblowers mandated under the Defend Trade Secrets Act. More information on the Vectrus Defend Trade Secrets Act policy may be found on the Vectrus intranet, by contacting an Ombudsperson, and at https://vectrus.com/dtsa-whistleblower-protections.

In addition, employees may use the Department of Defense Inspector General (DOD IG) Hotline at www.dodig.mil/hotline/hotlinecomplaint.html to report issues related to fraud, waste, abuse, and mismanagement for programs and personnel under the purview of the U.S. Department of Defense.

NOTES

VECTRUS

TRUE TO YOUR MISSION

655 Space Center Drive
Colorado Springs, CO 80915

719.591.3600

VECTRUS.COM