KFORCE℠

WE LOVE WHAT WE DO
WE LOVE WHO WE SERVE®

COMMITMENT TO INTEGRITY

You are our Firm's most valuable resource. Together, we have a long history of achieving Great Results. How we achieve these results matters, as does our commitment to protecting them. Nothing is more important to our Firm and its success than our Core Values. By living our values, we protect the results we achieve and the culture we have all worked so hard together to create. Our culture is what differentiates us. We have a long legacy to live up to, and each and every representative of Kforce is responsible for guarding our culture for those who will come after us.

The pages that follow are about those Core Values and what they mean to our culture. It is our Commitment to Integrity. Please take time to read it. If there is anything you don't understand, please ask your leader about it, or feel free also to talk with Human Resources.

We expect each member of the Kforce family to live our Core Values every day through words and actions. Over the many years our Firm has been in business, we have established a foundation of trust with each other, our clients, and our communities, and it's up to each of us to protect this reputation.

Thank you for being our partners in honoring this Commitment.

Very truly yours,

Dave Dunkel, CEO and Chairman Joe Liberatore, President

TABLE OF CONTENTS

OUR HISTORY, OUR CULTURE, OUR VALUES

Kforce, an abbreviation for KnowledgeForce®, describes our heritage and stands as a representation of our business model. "Knowledge" signifies both the skilled professionals we staff and the knowledge our Firm has gained through years of industry experience. "Force" symbolizes the strength of our team and cohesive efforts to provide valuable services and solutions. For over 50 years, we have matched candidates and clients, and have created a full circle staffing business. Our Firm is built upon a foundation of ethics, integrity, honesty, professionalism, fair business practices and compliance.

We are committed to act with integrity towards each other, communicating openly with one another, treating each other fairly and with professionalism and respect, and maintaining a safe and productive workplace.

We act with integrity with our clients and other partners exercising fair business practices, avoiding corruption, and avoiding conflicts of interest (among others).

We are committed to the communities we serve and, charitable and civic engagement and environmental stewardship, are of utmost importance to us.

We have an obligation to act with integrity and to reinforce our Core Values in everything we do and we have a personal responsibility to understand and adhere to this Commitment. Keep in mind also that many of the principles described in this Commitment are general in nature. We do not specifically address every situation or circumstance that might arise in the course of business. It is up to each of us to act using common sense, refer to other available resources, and to seek guidance when necessary.

The Kforce Commitment to Integrity is applicable to all officers, associates, consultants, suppliers, contractors and business partners of Kforce Inc. and its subsidiaries, the Kforce Inc. Board of Directors, and anyone authorized by Kforce Inc. to act on its behalf. In honoring these commitments in our day-to-day business decisions and interactions, we also serve our shareholders. Please understand that violations of our Commitment to Integrity may result in disciplinary action up to and including termination of employment or any other relationship you may have with our Firm.

CORPORATE DISCLOSURES

It is our policy to make full, fair, accurate, timely and understandable disclosure of our financial affairs in compliance with all applicable laws and regulations in all reports and documents that we file with, or submit to, the Securities and Exchange Commission and in all other related public communications made by us. Our officers are required to honor this policy in all respects; to promote compliance with this policy by all employees; and to abide by all of our standards and procedures which are designed to promote compliance with this policy.

WHAT WE EXPECT OF OUR LEADERS

Our Core Values are only successful when they are embraced and displayed by our leaders, starting at the very top. We place special trust in our leaders to guide our Great People and, as a result, we expect our leaders to hold themselves to the highest standards of accountability. We expect our leaders to:

- Lead by example
- Help associates understand this Commitment, including ensuring annual training is completed
- To be available to help answer associate and consultant questions about this Commitment
- To create an environment where associates feel comfortable raising concerns
- To promptly investigate and address concerns that are raised with them about potential violations of this Commitment
- Take prompt action when there is knowledge of violations of this Commitment

WAIVERS

Our Commitment applies equally to all Kforce employees, consultants, and others acting on our Firm's behalf. In the unlikely event that granting a waiver from any provision of this Commitment is in our Firm's best interests such a decision may only be made by our Legal Department and the CEO, President, or the CFO. Any waiver of this Commitment for executive officers or directors may be made only by the Kforce Inc. Board of Directors or its designated committee, and shall be promptly disclosed to the extent required in accordance with the rules and regulations promulgated by the SEC and Nasdaq.

COMPLIANCE WITH LAWS

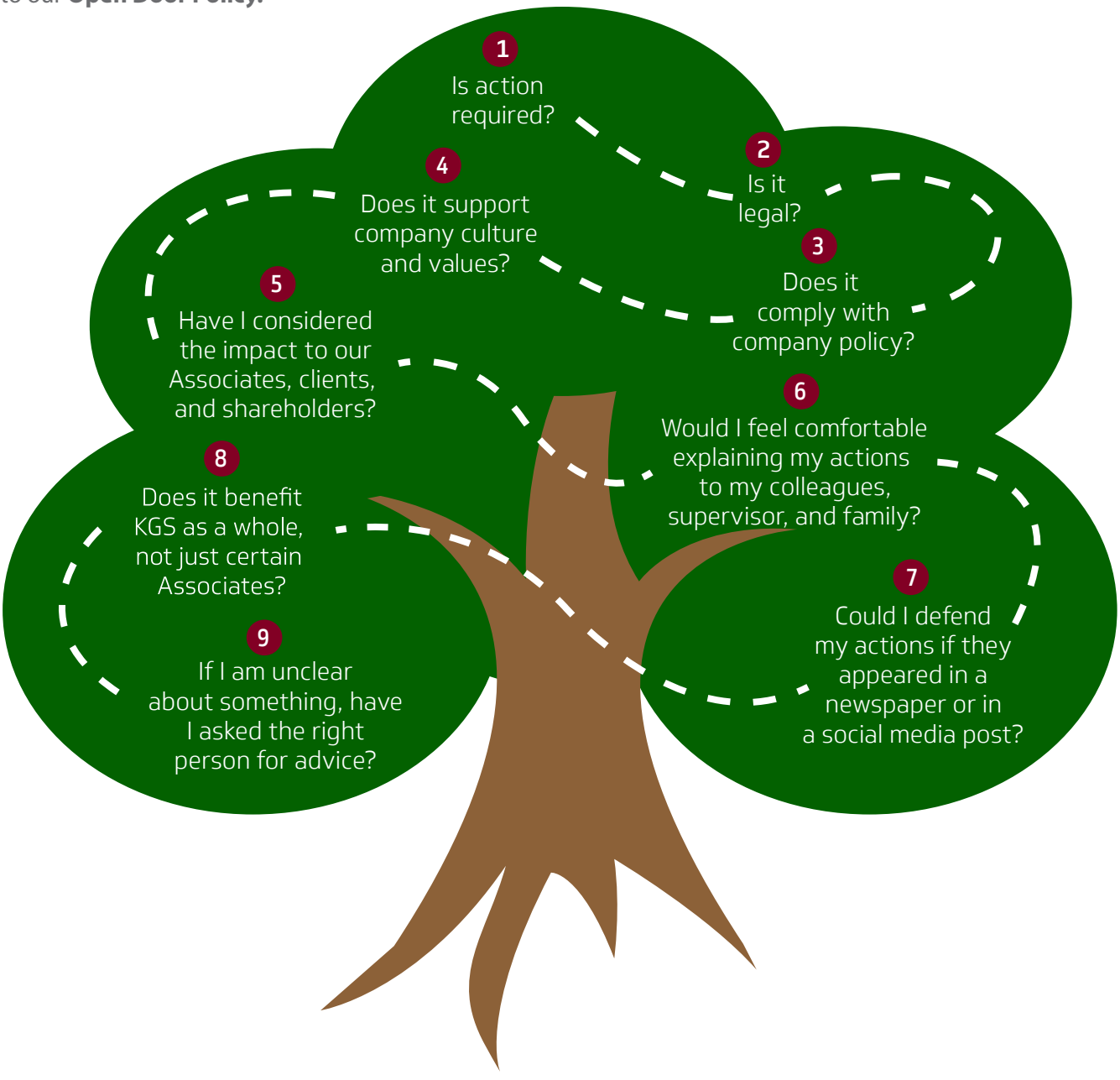
It is our policy to comply with all laws, rules and regulations applicable to our business or operations. We expect everyone covered by this Commitment to follow and comply with all such applicable laws, rules and regulations.

OUR DUTY TO SPEAK UP & ASK QUESTIONS

Speaking up when something's not right is not only our duty, it is also a part of building a culture of respect, integrity and trust. We know coming forward with concerns and asking questions about the right thing to do takes courage so we are committed to handling your concerns discretely and with care. We will also not retaliate or permit retaliation against anyone raising a concern in good faith.

In general, it is our hope that you will feel comfortable raising any concern you have with your leader. We realize, however, that there may be some things that you feel uncomfortable bringing to your leader and in those situations, we encourage you to raise your concerns using one of the other options available to you.

No matter who you contact know that you are doing the right thing by speaking up and asking questions. For more information, please refer to our **Open Door Policy.**



- Your leader
- To your leader's supervisor
- Human Resources

Customer Solutions Center at corphelpdesk@kforce.com or 866.807.5074

Internal Audit Department at 813.552.2761

OUR INTEGRITY HOTLINE

You can always raise concerns using our hotline.

866.213.5142

The hotline is administered by an independent third party. You can make reports to the hotline anonymously but we strongly encourage you to identify yourself when making a report to the hotline so we can to more thoroughly investigate your concern.

In order to fulfill our mission To Have A Meaningful Impact On All The Lives We Serve[SM], respect must be at the forefront of every decision, business transaction, interaction, and communication that we make. Demonstrating respect requires that we seek to understand how others see the world around them and that we withhold judgement and biases. The very definition of respect means, that we have true regard for the feelings, rights, wishes and the traditions of others.

Having respect for the diverse ideas and opinions around us is what unites us. Moreover, showing respect reduces stress and conflicts and increases productivity and knowledge, since it allows us to be open and collaborate with one another. Our culture is driven by respect and appreciation for each other, our clients, our candidates and business partners, so we must commit ourselves to demonstrating respect in all we do.

FAIR TREATMENT & EQUAL OPPORTUNITY

We believe that a diverse workforce made up of team members who bring a variety of skills, experiences and backgrounds is essential to our success. We are committed to fair treatment and equal employment opportunity. We do not discriminate against any protected class and this Commitment extends to all employment activities and decisions.

We also provide reasonable accommodations when a physical or mental condition requires such accommodations. Associates and consultants who believe they could benefit from an accommodation should request one through Human Resources or their leader.

If you believe you have been discriminated against or you witness discrimination against others, you must report it using one of the options in the "Speak Up" section. This also applies if you believe one of our clients, vendors or other business partners is discriminating against you or others.

PROFESSIONALISM & RESPECT IN THE WORKPLACE

For more information, refer to our **Professionalism and Respect in the Workplace Policy.**

Race, color, religion, creed, gender, sex, sexual orientation, gender identity, gender expression, age, disability, pregnancy (or related medical condition), national origin, genetic information or ancestry, military or veteran status, domestic violence victim status, protected activity (such as opposition to or reporting of prohibited discrimination or harassment), as well as citizenship, martial, veteran, and family medical leave status, or any other status protected by state or federal law(s)

HARASSMENT & BULLYING

We strive to maintain a work environment free from harassment and bullying. Harassment can include any behavior that creates an intimidating, offensive, abusive, or hostile work environment. Harassment can be sexual or non-sexual in nature, and can include things like:

+ verbal comments, such as slurs, offensive comments, and jokes;
+ physical contact, including unwelcome touching, hugging, massaging, assault, or intimidation;
+ visual displays, such as offensive photographs, videos, and drawings; or
+ electronic statements, such as bullying or stalking on social media or text messages.

Unlawful harassment includes harassment based on any protected class. To be clear about it, though, our Commitment goes beyond simply what the law may define as "harassment," "bullying," or "hostile work environment." Our Core Value of Respect requires us all to adhere to high standards of professionalism, respect, and civility toward each other and toward our business partners.

SAFETY & VIOLENCE PREVENTION

It's important that we work together to maintain an environment that is healthy and safe. All associates and consultants must follow safety policies and procedures that apply to them, obtain all required safety training and certifications, and, if necessary of their position, use personal protective gear as required.

In addition, violence or threats of violence in the workplace, or outside the workplace if it could affect someone's ability to work, are strictly prohibited. Examples of conduct that might be violent or threatening include but are not limited to, actual or potential assault, battery, intimidation, threats, stalking, bullying, destruction of property, or any similar act that occurs while an individual is engaged in Firm business, at a Firm or client site, or while attending a Firm-sponsored event.

Dangerous or illegal items of any nature such as weapons, explosives, or firearms are not permitted on Firm or client property. Individuals with authorized permits or licenses may have firearms or weapons in their locked vehicles in parking areas where allowed by law. Even with conceal carry permits, weapons and firearms are not permitted in Firm offices unless you have pre-registered and obtained written approval from Kforce Security Services. Certain locations may have more restrictive prohibitions based upon local laws and we must obey the law where our offices are located. In addition, certain security personnel retained by the Firm may also be authorized to carry firearms or other protective weapons as appropriate for their position and as permitted by law.

All associates and consultants should monitor their surroundings and must report any unsafe conditions or behaviors, no matter how minor, to their manager, account executive, or another leader as appropriate. For more information, refer to our **Safe Work Environment Policy.**

SUBSTANCE ABUSE

We want to provide safe and reliable services to our clients and a productive, healthy and, safe work environment for all associates and consultants. Being under the influence of drugs or alcohol on the job can compromise our interests and endanger your health and safety as well as the health and safety of others. The use, possession, sale, or distribution of illegal and/or controlled substances, other than as prescribed by a medical doctor, and alcohol on Firm or client property, except as specifically authorized by the Firm or client is strictly prohibited. You should never come to work under the influence of drugs, alcohol, or any controlled substance that could impair your ability to make sound judgments and perform your duties. For more information, refer to our **Alcohol and Drug Free Workplace Policy.**

WAGE & HOUR

We want everyone to be fairly compensated for all time worked, and we are committed to following the laws concerning hours worked and fair pay, including payment of overtime and minimum wage. To honor this commitment, accurate and honest timekeeping and reporting is required. Associates are required to report all hours worked during each reporting period. For more information, please refer to our **Timekeeping and Fair Pay Practices and our Meal and Breaks Policy.**

TRUST

Trust is the foundation of every relationship – whether personal or professional. Our business is built on relationships. Our consultants trust us with their careers and our clients trust us with their future plans and business needs. Additionally, we trust our associates, consultants and business partners with our information and resources. Trust is fundamental at all levels, from leadership to associate, associate to managers, from department to department and coworker to coworker. We inspire trust through actions and words. This means that we demonstrate care and responsibility with what we are entrusted. Our commitment to trust will ensure we maintain our long-standing relationships and our continued success.

INFORMATION & TECHNOLOGY RESOURCES

We rely on Firm information and technology resources to help us with our work. Information and technology resources include but are not limited to, e-mail, computers, software, networks, internet, telephones, mobile devices and voicemail systems. These resources are provided to conduct business and must never be used for illegal or inappropriate purposes. You should also know that any information saved or transmitted through our technology systems is our property and may be subject to inspection, retention, and review by Kforce, with or without an employee or third party's knowledge, consent, or approval.

Consultants must also abide by the policies of our clients when using any information or technology resources to perform work for our clients including when you are using your own equipment for such work. Remember, when using Firm equipment and systems, always conduct yourself professionally and courteously. For more information, please refer to our **Acceptable Use Policy.**

THEFT & FRAUD

Preventing and detecting theft and fraud is critical to protecting our Firm and fostering our Core Value of Trust. Intentionally concealing or misrepresenting facts to deceive or mislead others is not permitted. Theft and fraud can include, but is not limited to:

- misuse, manipulation, or lobbying for positive outcomes on internal or external client or candidate satisfaction surveys;
- falsely representing sales or other reports;
- manipulating internal reporting codes;
- falsifying timecards or any other company document;
- back-signing forms or agreements; or
- offering unauthorized discounts.

If you suspect any act of theft or fraud, immediately contact your leader or report the matter as directed in the "Speak Up" section of this Commitment.

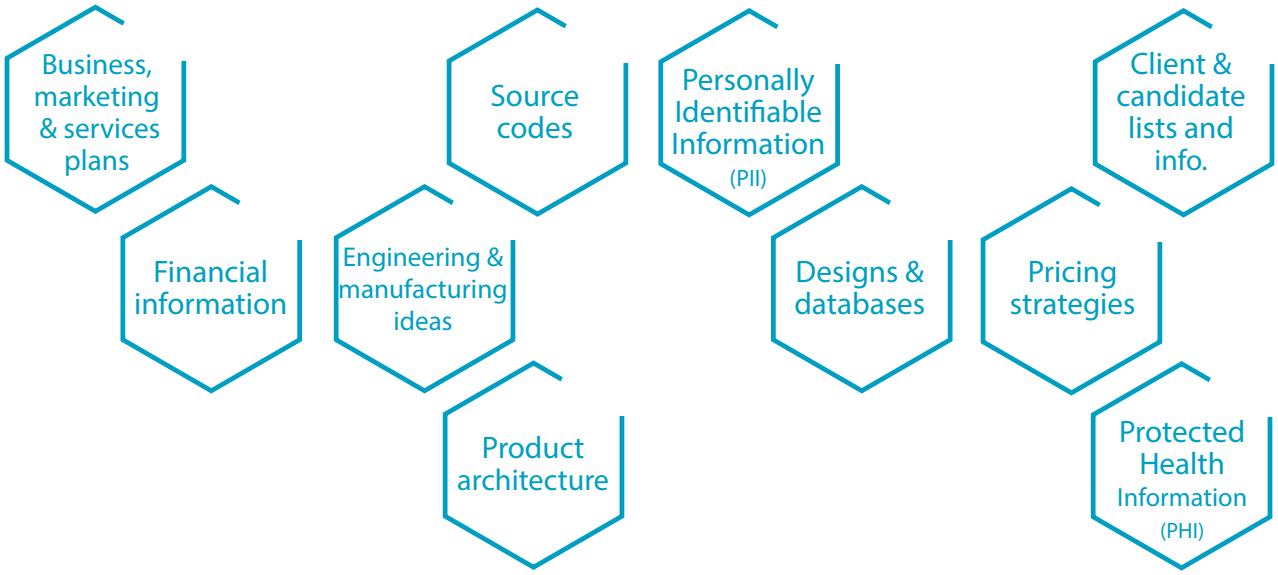
PROPRIETARY & CONFIDENTIAL INFORMATION

Many details about how we and our clients do business need to remain confidential for us to be competitive and successful. You may learn confidential or proprietary information about our Firm, our clients or other business partners when performing work duties. Confidential information should only be used for legitimate work purposes and you must maintain the confidentiality of all information entrusted to you, even after you stop working with or for us.

Additionally, you should respect the rights of and your obligation to former employers who may have entrusted you with their own confidential information. You should never use a former employer's confidential and proprietary information in violation of any employment or other agreements you may have had while working with them.

Confidential Information includes non-public information that might be of use to competitors or harmful to our Firm or its customers if disclosed.

CONFIDENTIAL INFORMATION INCLUDES



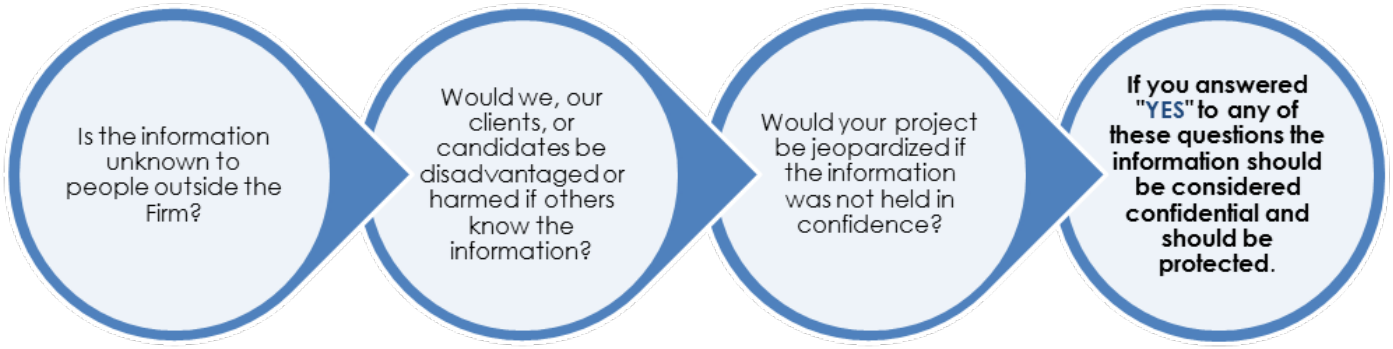
ALSO, ANY SIMILAR INFORMATION PROVIDED TO US BY OUR CLIENTS OR BUSINESS PARTNERS.

Please take care not to inadvertently disclose confidential information. Securely store materials that contain confidential information such as memos, notebooks, laptop computers, and mobile devices. Firm e-mails, voicemails and other communications containing confidential information should not be forwarded or sent outside of Kforce except for legitimate business purposes.

Please note, however, that we recognize and protect your rights to report potential violations of law to appropriate authorities. You may disclose confidential information and trade secrets in confidence, either directly or indirectly, to a federal, state or local government official or to an attorney solely for reporting or investigating a suspected violation of law. Confidential information and trade secrets may also be disclosed in a complaint or other document filed in a court proceeding, but only if the filing is made under seal. Additionally, if you file a retaliation lawsuit for reporting a suspected violation of law, you may disclose related trade secrets and confidential information to your attorney and use the information in court proceedings if the document is filed under seal.

We have a responsibility to recover and prevent unauthorized disclosure of confidential information. If you discover or suspect that confidential information is being used or disclosed inappropriately, please notify us through one of the options listed in the "Speak Up" section.

IS IT CONFIDENTIAL INFORMATION?



INTELLECTUAL PROPERTY

Our intellectual property is among our most valuable assets. We value and encourage the protection of our intellectual property while also respecting the intellectual property rights of others. We protect intellectual property from illegal or other misuse by making sure it is marked with the appropriate trademark, service mark, copyright notice or patent. To avoid infringing on the rights of others, do not:

+ Use Kforce resources or time to create or invent something unrelated to our business;
+ Use a previous employer's intellectual property without that company's permission;
+ Make unauthorized copies of or download software or license information, without appropriate permission; or
+ Affix the trade or service mark of another company to any Kforce materials without authorization.

Make sure to notify your leader of any innovation developed on Firm time or the use of Firm information or resources so that we can determine if we need to pursue formal legal protection of the intellectual property.

WHAT IS INTELLECTUAL PROPERTY?

Copyrights
Patents
Trademarks
Trade secrets
Design rights
Logos
Expertise
Consultant and client information
Kforce systems, including Recruitmax
Work product

WHAT IS WORK PRODUCT?

Things that are created by our associates or consultants as part of their work duties and/or using Kforce or client information or resources.

Work product is the property of Kforce or if the work is performed for one of our clients, the work belongs to our client. Work product includes:

- Inventions
- Discoveries
- Ideas
- Improvements
- Software
- Artwork
- Works of authorship (i.e. books, articles, brochures, etc.)
- Presentations (PowerPoint or other formats)
- Forms and checklists
- Strategic plans
- Training materials

Questions? Contact our Legal Team

PRIVACY

We respect the privacy of our associates, consultants, business partners and clients, and we are committed to handling their personal information (also referred to as Personally Identifiable Information or "PII") with care. While conducting business, we may collect personal information about our associates or have access to the personal information of our clients' employees, customers or business partners. This could include names, addresses, telephone numbers, marital status, health information, governmental identification numbers, financial information or other sensitive personal identification data. If you work with or encounter personal information, you have a duty to protect its privacy – even after you leave our Firm. You are also required to report any suspected breach immediately. For more information, please refer to our **PII Handling and Breach Incident Policy.**

INSIDER TRADING

When we have access to business information that others don't, we cannot trade Kforce or client stock based on that information. All consultants, associates, contractors and others having access to our confidential business information are prohibited from trading or enabling others to trade Kforce stock or stock of a customer, supplier, competitor, or potential acquisition while in possession of material non-public information ("inside information") about that company. Material information is any information that an investor might consider important in deciding whether to buy, sell, or hold securities. Information is considered non-public if it has not been disclosed to the public. Information is not considered public until the second trading day after it has been disclosed to the public. Not only does it violate our policies to use material non-public information to buy or sell securities, including 'tipping" others who might make an investment decision based on the information, but it is also illegal and can lead to substantial fines and imprisonment. Please make sure you are familiar with and follow our **Insider Trading Policy.**

The Core Value of Integrity is woven into this entire Commitment and each of our values. We hold ourselves to high moral principles and strive to do the right thing in everything we do. Integrity requires us to be transparent and truthful in all we say and do. Integrity is visible through our actions, words, decisions and methods. Our Commitment To Integrity is fundamental to our business and to the very core of who we are.

ACCURATE RECORD KEEPING

Accurate and reliable records are crucial to ensuring we conduct business lawfully. Records preserve our corporate memory, help us fulfill our financial commitments and are the basis for reporting our results to the government, the public, and our investors. We all contribute to our data integrity in some way and must ensure we create and maintain true and accurate records. Records include but are not limited to:

- timesheets and invoices
- expense reports and receipts
- accounting, tax and financial data
- employment records
- contracts
- electronic data files

We must also keep our records in compliance with our **Records Retention Policy.** When documents are needed for an investigation, audit, or potential lawsuit, they may be placed under a legal hold. If you receive notice of a legal hold, normal record retention schedules will not apply to any document or information covered by the hold, and you must help us retain the records until the hold is lifted. You cannot damage, alter, or destroy any materials on a legal hold until you receive a notice from our Legal Department stating that the hold has been lifted.

If you have reason to believe that records are not being created and maintained in accordance with this policy you must report it immediately through one of the avenues listed in the "Speak Up" section. Further, you must report any attempt to pressure you to prepare, alter, conceal or destroy documents in violation of this policy.

CONFLICTS OF INTEREST

Avoiding conflicts of interest is critical to honoring our Commitment to Integrity. A conflict of interest can happen when your personal interests or activities outside of the workplace or those of a close family member are, or may be, in conflict with the interests of Kforce. As associates, consultants, leaders or business partners of Kforce, we have a duty to make business decisions in the best interest of the Firm without the influence of personal interests or gain.

One of the concerns with conflicts of interest is that they can encourage you to show favoritism toward a person or organization at our Firm's expense. Even if that is not the case, the appearance of favoritism can undermine your decisions. The key to avoiding conflicts of interest is transparency. By disclosing the nature of your relationships we can take steps to have decisions reviewed by independent decision-makers who are free of conflicting interests. Accordingly, if you believe you have a conflict of interest situation, disclose it to your manager or Kforce's Legal Department immediately. Your manager and our Legal Department can help you resolve the conflict.

Outside Directorships

Serving on outside boards, either for-profit or non-profit, can present conflicts of interest, especially when the organization is a competitor, client, supplier or other business partner. Before accepting membership on any board, it is important to understand your legal responsibilities and avoid affiliations that carry the potential for distraction and conflicts of interest. In addition, service on outside boards may require pre-approval. For more information, please refer to our **Conflicts of Interest Policy.**

Family and Friends

A conflict of interest or favoritism can also arise when two associates have a close personal or family relationship – especially if they share a reporting relationship. Our policy is to prevent this from happening. You should not be placed in a position where you have direct decision-making authority over a family member, or vice versa. Similarly, managers should not date or pursue romantic relationships with their reports. All of us must follow the requirements of our **Fraternization and Nepotism Policy.**

Endorsements

Sometimes a third party will ask us for an endorsement or for permission to use our brand or logo in their materials. They might also request to use quotes from our business leaders or ask that one of our representatives appear for a speaking engagement. While an endorsement might appear wise at the time it is issued, future actions of the person or organization being endorsed may damage its reputation – and that, in turn, could damage our reputation. Because of these risks, we only allow endorsements in rare circumstances. If you are approached with a request for an endorsement or a speaking engagement where you will be asked to speak on our behalf, please ensure you have consulted with our Legal Department before agreeing to the endorsement or committing to speak. They can work with you to make sure the Firm's interests are protected and that all appropriate approvals are obtained.

Gifts and Entertainment

We must ensure that our gifts and entertainment could never be perceived as being given in anticipation of receiving favors or preferential business treatment. All associates and consultants are prohibited from offering and/or accepting a gift, favor, or entertainment in connection with their work if it is:

- cash (recognition gift cards, are permitted up to $100)
- inconsistent with customary business practices
- extravagant or extremely valuable
- is or can be perceived to be a kickback or bribe in violation of any law
- is in violation of any applicable law or regulation

GIFT= anything of value
vacations, tickets, endorsements, gift cards, tangible goods

ENTERTAINMENT = an experience given for leisure or amusement where both parties are present. Admission to an event when one of the parties is not present is a gift not entertainment.
meal, event, ball game

What can I offer?

When offering gifts or business entertainment, we must ensure that:

- gifts are valued at no more than $100
- entertainment is reasonable and modest in value (generally, not to exceed more than $100/person without prior written approval of your office leader)
- gifts are professional and tasteful
- gifts are consistent with any policies our business partners place on receiving gifts and entertainment
- they are unsolicited (i.e. the business partner did not ask for or suggest it)
- business is discussed during the entertainment and entertainment takes place in a setting that is appropriate for business discussion
- whatever we offer does not violate applicable contracts, laws and regulations

What can I accept?

We may only accept gifts and entertainment that are:

- Valued at no more than $100
- not cash or cash equivalents (such as gift cards)
- customary, tasteful and infrequent
- unsolicited
- for a business purpose
- infrequent, reasonably priced business meals
- in compliance with applicable contracts, laws and regulations

IMPORTANT: Offering gifts, meals, or entertainment to government employees is more strictly regulated. Accordingly, we prohibit giving any gifts, entertainment, or meals to government officials – although you may provide light refreshments for business meetings with government officials.

IMPORTANT: Before accepting any gift or entertainment, you must report the offer to your manager. In addition, any gift or entertainment that is not permitted as outlined in this section – whether given or received – must be approved in writing in advance by your Senior Leader.

PREVENTING CORRUPTION

Bribery and kickbacks – whether to governments, other businesses, or any individual – are never acceptable. Associates, consultants, or anyone else acting on our Firm's behalf must not offer or provide bribes, kickbacks, or other improper benefits to obtain an unfair advantage in business. For purposes of this policy, a bribe is defined as directly or indirectly offering anything of value to influence, persuade or secure an unfair advantage. This includes such things as: cash, gifts, entertainment, meals, travel and lodging, personal services, charitable donations, business opportunities, favors, offers of employment.

The Foreign Corrupt Practices Act (FCPA) and other U.S. and international laws prohibit payment of any money or providing anything of value to a foreign official to influence any business decision. Foreign officials include:

- any foreign government, including any department, agency, military branch, court or legislature
- any partially or wholly owned government entity such as a nationalized corporation or industry
- any political party, including party officials or candidates
- employees of public international organizations or any of their departments or agencies (i.e. World Bank, Red Cross)

Facilitation payments are payments that may be requested in foreign countries for obtaining ordinary licenses, work permits, visas and other similar customary governmental services. Prior to agreeing to or making any such payment, associates or others acting on our behalf must obtain express approval from our Legal Department.

COMMUNICATING WITH EXTERNAL PARTNERS

Integrity requires that we communicate with the public fairly and with a consistent voice. Be careful that in any communication that might become public, you do not appear to be speaking or acting on behalf of the Firm unless you have been specifically authorized to do so.

Communications that might become public include but are not limited to online forums, social media sites, interviews with journalists and television reporters, and bulletin boards. If you receive a call from a reporter or media outlet and you are asked to speak about a public issue on the Firm's behalf, politely decline the request and refer the person calling you to the Corporate Communications Team for response. For more information, refer to our **Media Communications Policy.**

WORKING WITH GOVERNMENTS

This section is intended to educate our associates and remind us that when we work in support of government, including the United States Federal Government, either as a direct supplier or a subcontractor, we are subject to rules that govern the procurement process. While our Commitment to Integrity applies equally across all our businesses, the following are just a few of the areas where working with governments requires us to honor several unique rules and obligations.

Conflicts of Interest

Individuals who have worked as a governmental employee may be subject to restrictions on their future business or employment-related activities within their former agency or department. The rules are very complex and agencies often have different interpretations of what is permitted under the rules. So, prior to engaging a former governmental employee – or if you are a former government employee – please remember to honor all restrictions that apply to engaging on contracts, programs, or with departments you or they supported while a government employee. If you are uncertain whether hiring a former government employee is appropriate, or if you are unsure about whether your assignment may violate the rules regarding personal conflicts of interest, please contact our Legal Department for guidance.

Organizational conflicts of interest can arise when work performed by a contractor's business with the government creates the potential for an unfair competitive advantage or may impair the business' ability to be objective in performing other tasks in support of the government. There are three types of organizational conflicts of interest: 1. Unequal access to information; 2. Ability to set biased ground rules; and 3. Impaired objectivity.

If you think any of these types of conflicts may apply, please contact our Legal Department for guidance.

Procurement Integrity

Every federal procurement is subject to the Procurement Integrity Act that establishes the level of interaction which the contractor may have with federal government employees during a purchase of goods or services by the federal government. Several state and local governments have similar laws. These laws prohibit contractors from intentionally obtaining contractor bid or proposal information or information about how the government is going to select the contractors who will win the award. If you happen to learn about either type of information, you should report it immediately to the Legal Department so you can receive guidance on how to handle the information.

Gifts and Gratuities

The rules against government employees accepting gifts and gratuities are very strict. So, it is our policy to prohibit the giving of any gift or gratuity to any government employee. As described earlier, a gift is anything of value including but not limited to a discount, entertainment, travel and transportation, cash, or a meal. You may however, offer light refreshments during a meeting to which government employees are invited. If you have any question about what qualifies as a gift or gratuity, please ask your manager, leader, or the Kforce Legal Department.

False Claims and Statements

As stated earlier, accurate and reliable records are crucial to ensuring we conduct business lawfully. When we support the government, it is very important that we can completely rely on the accuracy and completeness of our records, including timesheets, invoices, and inventories. If we fail to submit accurate invoices, timesheets, or other claims for payment we may face civil and criminal liability under the False Claims Act or other similar state and local laws. In addition, we may be in breach of our contracts, and that could result in termination of our client relationship, damage to our reputation, and impair our ability to win new government contracts.

If there is any reason to believe that records are not being created and maintained in accordance with this policy you must report it immediately to your manager, our Integrity Hotline, or through some other avenue listed in the “Speak Up” section above. Further, you must report any attempt to pressure you to prepare, alter, conceal or destroy documents in violation of this policy.

When it comes to service, we want to be the exception, not the rule. Our commitment to Exceptional Service means we go above and beyond what is expected. It also means that we are ethical in our business practices and work with ethical partners. Demonstrating Exceptional Service requires that we are: compassionate - by putting ourselves in the shoes of others; solutions driven - by proactively helping to solve problems or need; always timely; and attentive to the needs of others.

Being committed to Exceptional Service will ensure we build meaningful relationships with each other, our clients, candidates and business partners.

ETHICAL PARTNERS

We are committed to conducting business ethically and morally. We expect the same of our business partners. As part of this Commitment, our Firm will not knowingly do business with anyone engaged in pursuits that we consider to be immoral or unethical.

ETHICAL SALES PRACTICE

Our vision is To Have A Meaningful Impact On All The Lives We Serve[SM]. This starts with ensuring that we establish and maintain an ethical sales culture. Many of the concepts outlined in this Commitment are the foundation to those ethical sales practices. We hold ourselves to the highest standards of Respect, Trust, Integrity and Exceptional Service in all business relationships. When selling our services, the needs of our clients and candidates must come first. We should offer solutions that are in the best interest - and address the opportunities, of each individual business partner, rather than seek our own personal gain. Additionally, business leads are to be obtained through approved, legitimate and legal sources. Cutting corners or compromising compliance requirements to earn a commission will not be tolerated. If you have questions about our sales practices, please contact your manager or use one of the options listed in the "Speak Up" section.

Honest Advertising and Marketing

Our commitment to Exceptional Service requires that we deal with our clients and business partners honestly and fairly. It is our responsibility and policy to accurately represent the Firm and our services in our marketing, advertising, and sales materials. Deliberately misleading messages, omissions of important facts, or false claims about our services, successes, and competitors are prohibited. Representations in our marketing and sales materials must be fact-based and accurate.

Competitive Information

Gathering information about our competitors and customers helps us make good business decisions. Such information must be gathered in appropriate ways, however, and not through using unethical, dishonest, or illegal methods and means. Appropriate methods for gathering competitive information include but are not limited to: publicly available sources such as the internet, news sources, industry surveys, competitor marketing materials, and customer interviews.

ANTITRUST & FAIR COMPETITION

Antitrust and competition laws benefit us all by allowing us access to quality products, services, and talent at fair prices. These laws prohibit collusive or unfair business behavior that restricts free competition. We are never permitted to enter into agreements with competitors, regardless of whether the agreements are formal or informal, written or unwritten, regarding any of the following:

- Prices or pricing strategy
- Discounts
- Terms of our customer relationships
- Sales policies
- Marketing plans
- Customer selection
- Allocating customers or market areas
- Allocating candidates or agreeing not to recruit each others' employees
- Contract terms and contracting strategies

We must be particularly careful when we interact with any competitor employee or representative, especially at trade association meetings or other industry events. Under no circumstances should you discuss customers, prospects, pricing or other business terms with any competitor.

PROCUREMENT & FAIR PURCHASING

Our procurement decisions are based on total value - quality, service, and price. The price paid for goods and services purchased by us must fairly represent the value of the goods or services provided. Unless written approval is provided by the supplier and our leadership, payments must only be made to the organization or individual providing the service and with whom we have an agreement to purchase. We will not purchase goods or services from any supplier that supplies unsafe products or services or violates laws or regulations applicable to the supplier.

We recognize that as successful members of our communities, we have a responsibility to support the communities we serve and contribute to the common good. We have a comprehensive Stewardship and Community program in place that provides a structure for all the members of our Kforce family to get involved with their local communities as a part of their careers. We truly believe in the adage that "it is better to give than to receive" and will continue to hold strong to our commitment to these Core Values.

CHARTIABLE CONTRIBUTIONS & VOLUNTEERING

Our Core Values of Stewardship & Community commit us to supporting the communities we serve. Every year, we participate in a select group of humanitarian and charitable causes and events. When we choose to participate in a community or charitable project that utilizes limited associate or consultant time and Firm resources, we will let you know that the effort is officially Firm-sponsored. While we encourage associates and consultants to participate in charitable and humanitarian efforts, no one should use Firm time or resources to support the efforts, nor should anyone represent that he or she is acting on behalf of the Firm, unless approval is specifically granted by senior management. When promoting charitable contributions and events, we should follow the guidelines in our **Solicitation and Distribution Policy.**

POLITICAL ACTIVITIES & CONTRIBUTIONS

We encourage associates and consultants to exercise citizenship and fully participate in local, national and international political processes. However, you may not use your position to force or pressure others to make contributions or support candidates or political causes. Additionally, you must never use Firm funds or resources for political candidates, campaigns, or parties. This includes devoting work time to any candidate's campaign or political party and the use of any Kforce facility or property. Contributions to a candidate for elective office or a political party must be at your own expense and political activities you engage in must be on your own time.

ENVIRONMENTAL STEWARDSHIP

We understand that supporting our communities includes being good environmental stewards. While our industry may have a smaller environmental impact than others, we are committed to conducting business in an environmentally responsible manner. We encourage all associates, consultants and business partners to seek ways to proactively address our environmental impacts and ensure we are conducting business in compliance with all applicable laws and in a manner that is protective of the environment. Additionally, associates whose work directly affects environmental compliance must be familiar with the permits, laws, and regulations that apply to their work.

SOCIAL MEDIA

Social media provides opportunities for us to connect with our communities in ways that may not be found through traditional sources. Most of us participate in various forms of social media such as Facebook, LinkedIn, Twitter, and other similar platforms. Some of our associates and consultants even host their own websites and blogs. While there are many benefits to using social media, online communications are easily made public and, accordingly, social media communications can have a significant effect on our reputation.

Good judgement and respect for others and our Firm should act as our guide when communicating through social media. If you identify yourself as an associate or consultant, please be careful not to attribute your personal opinions or beliefs to Kforce. Unless you are authorized to speak on our behalf, do not make statements or announcements as a Kforce representative. For more information, refer to our **Social Media Policy.**

COMMITMENT TO THESE STANDARDS

Our culture is shaped by the values outlined in this Commitment, our Great People and our drive to work hard but have fun along the way. In order to preserve our culture, we must choose to hold firm these guidelines every day. This Commitment should serve as a road map to all we do. We understand, however, that it's not realistic to always remember everything that's outlined in this Commitment so if you find yourself in a situation where you're not sure what to do, please use one of the options available in the "Speak Up" section.

Our Compliance Program

We are all responsible for complying with this Commitment and we must hold each other accountable to the highest levels of integrity. However, our Commitment to Integrity is administered by our General Counsel and our Risk and Compliance Team. Our Risk and Compliance Team helps enforce this Commitment by ensuring it - and our policies - are up to date. The Commitment to Integrity is also endorsed by and has the full support of our Board of Directors. In addition to the "Speak Up" section, you can also contact the Risk and Compliance Team at ComplianceTeam@kforce.com if you have questions regarding the items in this Commitment.

Training

Our Risk and Compliance Team administers compliance training, including training on this Commitment. We provide training to our associates on many of the topics in this Commitment on an annual basis. All associates have a duty to complete the mandatory training.

INVESTIGATION

There are times we must look into situations that could involve a violation of this Commitment, one of our policies, or other misconduct. All of us have a responsibility to cooperate with Firm investigations, to treat those investigations with high discretion, and to be honest and forthcoming in those investigations. Failure to cooperate with an investigation can lead to discipline up to and including termination. You will never be subject to retaliation for your good faith participation as a complainant or witness about an investigation.

CONCLUSION

Thank you for sharing our Commitment to Integrity. While this Commitment does not create a contract of employment or alter anyone's at will employment status, honoring these policies will help us live up to our Core Values and our vision To Have A Meaningful Impact On All The Lives We Serve[SM].

Policy Name:	Professionalism and Respect in the Workplace (EEO, Anti-Harassment & ADA)	**Revised:**	10/01/2020
Applicable to:	All Kforce Employees, Companies & Locations	**Customer Solutions Center:**	1-888-435-7957, option 1, CustomerSolutionsCenter@kforce.com

Respect is a Kforce Core Value. We are committed to a fair workplace where employment and advancement are based on merit and business needs, and where all of our associates treat each other with respect. With this policy, we not only prohibit all forms of illegal discrimination, harassment, and retaliation, but we go further: all of our associates, consultants, contractors, vendors, and other business partners are expected to treat each other with professionalism and respect.

Equal Employment Opportunity and Affirmative Action

A diverse workforce made up of team members who bring a wide variety of skills, abilities, experiences, and perspectives is essential to our success. We are committed to providing equal employment opportunity. This commitment extends to all employment activities, including but not limited to recruiting, hiring, benefits, leaves of absence, training, transfer, promotion, job assignments, participation in company programs or events, compensation, corrective action, termination decisions. We do not discriminate based upon any employee's or consultant's race, color, religion, creed, sex, gender, sexual orientation, gender identity, gender expression, age, physical or mental disability, pregnancy (including childbirth, breastfeeding , or related medical condition), national origin, genetic information or ancestry, military or veteran status, domestic violence victim status, protected activity (such as opposition to or reporting of prohibited discrimination or harassment), as well as citizenship, marital, veteran, and family medical leave status, or any other status protected by local, state, or federal law(s). This applies not only to our decisions involving core associates of the Firm, but also to hiring, placing, and employing our consultants. For example, we will not screen candidates based on any discriminatory standard or an inappropriate or illegal qualifier, such as "no females," "no accents," or "young talent."

Kforce is an affirmative action employer and complies with applicable federal, state, and local laws and regulations concerning equal employment opportunity and affirmative action. As part of our commitment to affirmative action, we maintain affirmative action plans. A copy of our plan for veterans and individuals with disabilities is available for review in our Corporate offices during regular business hours. Our Affirmative Action Officer is responsible for coordinating and monitoring our affirmative action efforts. Any reports of concerns or violations of our affirmative action commitments should be reported to the Affirmative Action Officer or through the options listed in our Open Door Policy. Like all Kforce policies, this policy is supported by all Kforce leaders, including each member of our Executive Committee, including our Chairman and Chief Executive Officer.

Anyone who believes they have been discriminated against in violation of this policy, or who witnesses such discrimination against others, must report the situation to their manager, Human Resources, or one of the other avenues for raising concerns listed in our Open Door Policy. This applies not just to acts involving Kforce personnel, but also if you believe one of our clients or other business partners is discriminating against you or others.

Reasonable Accommodations

We also provide reasonable accommodations to employees and consultants whose physical or mental condition requires such accommodations. Qualified individuals who need an accommodation because of a disability or medical condition should contact Human Resources. Please let us know what type of accommodation you need, and know that we treat your accommodation request and related medical information as confidential. Accommodation and medical information is stored apart from your personnel record.

We are committed to engaging our associates and consultants who need accommodations in interactive dialogue to identify and remove the barriers that make it difficult to do their jobs.

In the same manner, we respect the sincerely held religious beliefs and practices of all employees and will make reasonable accommodations for sincerely held religious practices and observances that do not create undue hardship.

No Harassment or Bullying

We are committed to maintaining a work environment free from all forms of harassment and discrimination, whether based on race, color, religion, creed, sex, gender, sexual orientation, gender identity, gender expression, age, physical or mental disability, pregnancy (including childbirth, breastfeeding, or related medical condition), national origin, genetic information or ancestry, military or veteran status, citizenship, marital status, veteran status, family medical leave status, domestic violence victim status, protected activity (such as opposition to or reporting of prohibited discrimination or harassment),or any other status protected by local, state or federal law. Harassment, bullying, or inappropriate conduct of any type by a supervisor, manager, coworker, or a non-employee third party such as a client, contractor, vendor, or supplier is not tolerated at Kforce.

So there is no misunderstanding, we define harassment broadly. We've described how we define sexual harassment in detail below, but the same broad principles we express for our definition of sexual harassment will be applied to harassment, bullying, or abuse based on any other protected statuses listed above. Sexual harassment includes unwanted sexual advances, requests for sexual favors or visual, verbal or physical conduct of a sexual nature when:

- Submission to, tolerance of, or rejection of such conduct is made a term or condition of employment;
- Submission to, tolerance of, or rejection of such conduct is used as a basis for employment decisions affecting the individual;
- Such conduct has the purpose or effect of unreasonably interfering with an associate's work performance or creating an intimidating, hostile or offensive working environment.

Sexual harassment includes various forms of offensive behavior. The following is a partial list:

- Unwanted sexual advances;
- Offering employment or other benefits in exchange for sexual favors;
- Making or threatening reprisals after a negative response to sexual advances;
- Visual conduct: leering, making sexual gestures, displaying of sexually suggestive objects or pictures, cartoons or posters;
- Verbal conduct: making or using derogatory comments, epithets, slurs, sexually explicit jokes, comments about a person's body or dress;
- Verbal sexual advances or propositions;

- Verbal abuse of a sexual nature, graphic verbal commentary about an individual's body, sexually degrading words to describe an individual, suggestive or obscene letters, notes or invitations;
- Physical conduct: touching, assault, impeding or blocking movements; and
- Retaliation for making harassment reports or threatening to report harassment.

This policy applies to males who sexually harass, bully, or are abusive or unprofessional toward females or other males as well as to females who sexually harass, bully, or are abusive or unprofessional toward males or other females.

Duty to Report Violations and Commitment to No Retaliation

Everyone plays a critical part in ensuring the workplace is free from harassment, discrimination, and retaliation. If you become aware of harassment, discrimination, or retaliation, you must report what you know to a manager, Human Resources, or use one of the other avenues for raising concerns listed in our Open Door Policy. Additionally, you may report a violation to the U.S. Equal Employment Commission ("EEOC") or an equivalent state government agency. Failure to report violations of this policy that you experience or witness could result in disciplinary action up to and including termination of your employment or business relationship with Kforce. Supervisors or managers who observe or receive reports of violations of this policy must immediately report the situation to our Human Resources Department.

You have our commitment that all complaints will be handled in a timely and thorough manner and as discreetly as possible. We do our best to be fair to all parties involved. Only those people with a need to know or who are necessary for the investigation and resolution of the complaint will be involved or given information about the matter. Investigations are documented and tracked. To the extent appropriate, when an investigation is complete, we will share the results with those who have a legitimate need to know about the investigation outcome. If Kforce determines that this policy has been violated, remedial action will be taken. Appropriate action will also be taken to deter any future harassment, discrimination, or retaliation.

Furthermore, we will not retaliate or in any other manner discriminate against associates, consultants, or applicants who have inquired about, discussed, or disclosed their pay or the pay of another associate, consultant, or applicant. However, associates who have access to the compensation information of others should not disclose pay to individuals who do not already have access or a need to receive pay information, except when we have a legal duty to furnish the information, when it is in response to a formal complaint or charge, or for an investigation, proceeding, hearing, or action, including an investigation conducted by us. You also have our commitment that no one at Kforce will not harass, intimidate, threaten, coerce or discriminate against any individual because the individual has engaged in, or may engage in a protected activity or for reporting a concern under the policy in good faith. If you suspect retaliation, immediately report your concern using as many reporting avenues of our Open Door Policy as you feel comfortable using.

Kforce Oregon Employees and Consultants – Appendix A

Appendix A - Prohibiting Harassment for Kforce Oregon Employees and Consultants is applicable to employees who live and work in the state of Oregon. Please click here to access the appending policy.

Policy Name:	Alcohol and Drug Use	**Revised:**	04/12/2021
Applicable to:	All Kforce Employees (Core Associates and Consultants)	**Helpdesk Information**	1-813-552-2025 backgrounds@kforce.com

Kforce is committed to providing safe and reliable services to its clients and a productive, healthy, and safe work environment for all employees. Employees who are under the influence of illegal drugs or alcohol or who are misusing prescribed drugs on the job compromise our interests and endanger their own health and safety as well as the health and safety of others. Any employee in violation of this policy is subject to disciplinary action, up to and including immediate termination.

When working (whether on or offsite), while operating any Kforce or client vehicle, and when present on Kforce or client premises, employees are prohibited from:

- using, possessing, buying, selling, manufacturing or dispensing any illegal drug (to include possession of illegal drug paraphernalia and possession or use of marijuana even in jurisdictions where recreational and/or medicinal use is legal);
- being under the influence of alcohol or an illegal drug;
- possessing or consuming alcohol (except at approved social functions, and even then, only in moderation); and
- taking prescription drugs in any manner inconsistent with prescribed or recommended usage or that impairs your ability to safely and effectively perform job duties.

We may take appropriate measures to determine if prohibited substances or items are located or being used on Kforce or client property. Such measures may include, but are not limited to, the reasonable search of employees and employees' personal property, including vehicles, handbags, briefcases, etc., located on Kforce or client premises, where permitted by applicable law. Employees should have no expectation of privacy while on Kforce or client property and agree to cooperate with such reasonable searches as a condition of employment. Such searches may be conducted by either Kforce management or law enforcement authorities, as appropriate and in accordance with applicable law.

Employees must report to their manager or a Human Resources representative any observed or suspicious situations in which another employee is in a condition that impairs his or her ability to perform job duties or that presents a hazard to the safety or well-being of the employee or others. Upon a reasonable suspicion of a violation of this policy, employees may be required to undergo drug testing, which will be conducted at a designated testing facility through an assigned third party.

Applicants for some core and consultant positions may be required to take pre-employment drug tests. For core positions, Kforce will excuse positive test results caused by use of marijuana if (1) the applicant is in a jurisdiction that has legalized the use of marijuana for medical purposes, the applicant possesses and produces appropriate medical authorization for such use, and the applicant's use is consistent with his or her medical authorization; or (2) the applicant is in a jurisdiction that has legalized the use of recreational marijuana and the applicant's use is consistent with the laws of that jurisdiction. For consultant positions, Kforce will excuse positive test results caused by use of marijuana if the client's drug policy allows an exception for authorized medical marijuana use and the use is consistent with that policy, or if the client otherwise agrees to excuse the positive test result. In all circumstances, employees are prohibited from using, dispensing, administering, or otherwise ingesting marijuana when working (whether on or offsite),

while operating any Kforce or client vehicle, and when present on Kforce or client premises on Kforce property or in the workplace.

Applicants who are disqualified for employment due to a positive drug test result may not reapply for employment for a minimum of six months.

Any employee convicted of, or who pleads guilty or no contest to, any federal, state or local drug or alcohol offense must immediately report the offense within five days of the conviction or plea of guilty / no contest.

We encourage employees and consultants to seek assistance for substance abuse and dependency problems through our employee assistance program (EAP). Employees and consultants should contact HR or the EAP directly at 833-789-9882 for additional information. Participation in EAP services and any recommended treatment is confidential. If it has been determined that an employee or consultant is in violation of this policy, participation in EAP services does not preclude any disciplinary action.

Nothing in this policy is intended to interfere with employee rights regarding leave or reasonable accommodations for persons with disabilities. For more information, see the Professionalism and Respect in the Workplace and Time Off and Leave policies.

Open Door Policy
Proprietary & Confidential

Policy Name:	Open Door Policy	**Revised:**	08/17/2020
Applicable To:	All Kforce Employees, Companies & Locations	**Integrity Hotline Information:**	1-866-213-5142

Kforce values its employees – all associates and consultants – and we adhere to strict standards of compliance and ethics. If a matter arises that you would like to discuss, we want you to feel comfortable raising your concerns.

If you become aware of a violation of our Commitment to Integrity, a policy violation, or any other serious issue involving misconduct, you must report the matter using one of the channels below. In addition, you are welcome to raise any other matter that concerns you through any of the channels listed.

In general, it is our hope that you will feel comfortable raising any concern you have directly with your manager. We expect our managers at every level to maintain an open door to your concerns. We realize, however, that there may be some concerns that you feel uncomfortable raising with your leader. In such situations, we expect and encourage you to raise your concerns through any of the following channels:

- your designated Human Resources Business Partner;
- the Customer Solutions Center at CustomerSolutionsCenter@kforce.com / 866-807-5074;
- your manager's supervisor;
- the Internal Audit Department at 813-552-2761; or
- the Commitment to Integrity Hotline at 866-213-5142. This is a third-party administered service that allows you to raise any concern. You may even choose to raise the concern anonymously. Keep in mind, however, that we are often able to more thoroughly investigate and take more complete action on your concern when we have all the facts and can follow up for clarification.

We take your concerns seriously and will handle them discreetly and with care. We strictly prohibit retaliation against anyone raising a workplace concern in good faith. Our Firm is committed to all of our Core Values, including our Core Value of Integrity, and we ask you to help hold ourselves and each other accountable to these values.

Policy Name:	Acceptable Use Policy	**Revised:**	6/28/2021
Applicable to:	All Kforce Employees, Consultants, Companies & Locations	**Technical Support Information**	1-888-435-7957, option 2, technicalsupport@kforce.com

Our Firm provides a variety of Firm Technology Resources for you to perform your work. For your convenience, we also enable some associates and consultants to use their personal technology devices for work purposes. We are committed to protecting our associates, employees, consultants, candidates, clients, and the public from illegal or damaging actions and to ensuring that Firm Technology Resources are used for appropriate purposes consistent with our Core Values.

This policy explains your responsibilities when using Firm Technology Resources or your own technology devices for work purposes regardless of where you are working, including, but not limited to: a Firm facility, your home, a client facility, in a public location, or traveling.

Violations of this policy may result in coaching or discipline up to and including termination of employment and legal action if appropriate.

Contact Enterprise Security (itenterprisesecurity@kforce.com) if you:

- believe Confidential and Proprietary Information may be at risk,
- need to report suspicious activity or policy violations,
- have any questions about this policy, or
- need to request an exception to this policy.

Suspect your device has malware? Immediately take the following actions and then call Technical Support:

- Stop using the device
- Do NOT turn the device off
- Disconnect the device from the network, including VPN or turning off Wi-Fi
- Make no attempt to remove the malware
- Document symptom details and the time(s) of the occurrence(s)

Definitions

- **Confidential and Proprietary Information**: includes any non-public data or information owned by the Firm concerning its business and affairs that if improperly disclosed might be of use to competitors or harmful to the Firm, employees, consultants, or customers. Examples of the Firm's Confidential and Proprietary Information includes, but is not limited to: business, marketing and service strategies or plans; any financial information including forecasts, pricing strategies; technical information; source code; designs and databases; PII or PHI; client, candidate or consultant lists and Sensitive Personal Information; any information provided to the Firm to be held and protected under contractual obligations; and any other information that should reasonably be recognized as confidential or proprietary information belonging to the Firm. (Note: Confidential and Proprietary Information belonging to clients must be protected and secured according to this policy as well.)
- **Firm:** Kforce and its subsidiaries. If you are a consultant, the term "Firm" refers to the Firm and to any client, to the extent the client provides technology, computing, software, and online resources. If

- the client has any policies, rules or requirements that go beyond or conflict with this policy, the stricter provisions of either policy will govern.

  Firm Information: Covers all information in any form, electronic or physical, used to support the Firm's daily operations, business objectives, and strategic direction.

- **Kforce Employee Wireless Network:** Wireless network provided solely for employee personal devices when used by employees in a Kforce facility.
- **Kforce Guest Wireless Network:** Wireless network provided for use by candidate and guest devices when such devices are used in a Kforce facility.
- **Kforce Firm Network:** Wireless and wired (physical connection) networks intended solely for Firm-provided technology devices when used in a Kforce facility.
- **Messages / Messaging:** For the purpose of this policy, these terms apply broadly to email messages, text messages, Firm-provided phone and tablet messages, Jabber messages, Microsoft Teams messages, and all similar technologies.
- **Personal Information**: is inclusive of all PII, PHI and Sensitive Personal Information. It also means any information that can be reasonably linked to any one person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, physical addresses, email addresses, telephone numbers, other identifying numbers, any financial identifiers, biometric information, internet activity, geolocation data, and personal trends.
- **Personal Health Information (PHI)**: Protected Health Information (PHI) means any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.
- **Personally Identifiable Information (PII**): PII is information that can be used to identify, contact, or trace a unique living individual. PII can be electronic or in paper form. Although the definition of PII varies state-to-state, the typical definition is:
- The first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to the individual:
- Date of birth (month, day, and year)
- Social Security Number
- Driver's license number, federal or state-issued identification card number
- Financial account, credit, or debit card number (with or without any required security code, access code, personal identification number (PIN), or password) that would permit access to an individual's financial account
- **Sensitive Personal Information**: is inclusive of all PII and PHI and further entails: (1) personal Information that reveals (A) social security, driver's license, state Identification card, or passport number; (B) a consumer's account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) precise geolocation; (D) racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of mail, email and text messages, unless the business Is the intended recipient of the communication; (F) genetic data; and (2)(A) the processing of biometric Information for the purpose of uniquely identifying a consumer; (B) personal Information collected and analyzed

- concerning a person's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive Personal Information that is "publicly available" shall not be considered Sensitive Personal Information or Personal Information.

  Technology Resources: For the purposes of this policy, technology resources refer to all technologies or technical services, including on-premises, hosted, cloud-based solutions, and mobile applications, that are owned, managed, or utilized by the Firm to create, collect, analyze, process, store, manage, send, transmit, or receive information.

  Examples of technology resources include, but are not limited to, laptops, desktops, applications, cloud services (IaaS, PaaS, SaaS), websites, telephone systems, e-mail systems, mobile computing devices, wireless services, portable storage such as thumb drives, USB devices, printers (including faxes and scanners), video conferencing systems, internet access, servers, operating systems, and networks.

General

- **Work with Integrity**. We expect all of our associates and consultants to honor our policies, practices, and Core Values when using Firm Technology Resources and when using your personal technology devices for work purposes.
- **Personal Gain is Prohibited.** No one is authorized to use Firm Technology Resources for personal gain. This includes using Firm Technology Resources in connection with employment elsewhere or to conduct any non-Firm business.
- **Intellectual Property.** All intellectual property (that is, any copyrightable works, ideas, discoveries, inventions, patents, products, or other information created for the Firm) that you produce using Firm Technology Resources or your personal technology devices for work purposes is a work-made-for hire and, therefore, owned by the Firm.
- **Recording Interviews, Training, and Meetings.** Be aware of what you are recording and whether the content is considered Confidential and Proprietary Information.
- Recordings of interviews are classified as Sensitive Personal Information. Access to and sharing of the recorded interviews must be limited to need to know based on job responsibilities.
- Recordings of training may contain system screens that contain Confidential and Proprietary Information or there may be verbal instruction about Kforce internal processes. If they do, access to and sharing of the recorded training must be limited to need to know based on job responsibilities.
- Recordings of meetings are classified based on the information discussed. Be aware of what you are recording and whether the content is considered Confidential and Proprietary Information.
- **Physical documents.** Regardless of your work location - Kforce facility, your home, client facility, public work area, etc. - physical business documents containing Confidential and Proprietary Information must be protected from view and from physical access.
- Only print a document if it is absolutely necessary to execute a business process. Convenience is not a business need.

-
  - Retrieve the document as soon as it prints.
  - Securely store documents when you are away from your work area.
  - When a Confidential and Proprietary document is no longer needed, it must be shredded.

Personal use of Firm Technology Resources. We understand that associates and consultants occasionally use the internet and email at work to get updates on the latest scores, check the news, catch up on personal email, or send a personal lunch invitation to a friend. Personal use should never:

- Compromise the productivity of you or your colleagues and must be consistent with other policies such as Professionalism and Respect in the Workplace.
- Negatively impact Firm Technology Resources due to excessive use of resources like data storage space or network bandwidth with non-business videos, music, or other activities.
- **Do not bypass or disable security or install applications that do so**. Do not bypass or disable security controls on any Firm Technology Resources or a personal technology device used to access Firm Technology Resources. This includes but is not limited to:
- Disabling anti-virus protection, bypassing Multi-Factor Authentication (MFA) or the web proxy, modifying configuration settings, or bypassing any other security controls is strictly prohibited.
- Installing applications designed to bypass security monitoring and controls, such as internet anonymization tools (i.e., TOR), personal or unapproved VPN systems, keystroke loggers, network scanning tools, etc., is strictly prohibited.
- **Be safe while working**. Do not use Firm Technology Resources or personal technology devices for work purposes while driving, operating machinery, or in any other situation where you are distracted from the attention required of you to perform any given task safely.
- **Physical Security**. As the Firm's business model continues to evolve, you may see different types of personnel in your building, i.e., third parties, subcontractors, consultants. If you are unsure whether someone should be in your area of the building, ask your leaders for assistance. Remember verbal conversations, content on computer screens, and physical documents can include information that is not intended for everyone around you.
- **International Travel Pre-notification.** Using Firm Technology Resources or accessing Firm information while traveling internationally increases the risk of exposure to malware and data theft. The Firm continuously monitors attempts to access Kforce's network and systems from outside the United States. Due to security concerns, access from some countries is blocked.
- Notify Technical Support before traveling internationally if you plan to work or access Technology Resources. This includes your personal mobile device when it is configured to access Kforce Technology Resources.
- If you do not notify Technical Support and connect to Kforce Technology Resources from nonUS locations, your account will be disabled.

•

Information Protection

Our Firm Information is critical to our success, and it is important for everyone to understand how to protect it. You are obligated to the following as it relates to all Firm data and information, whether in a Technology Resource or hard copy:

- **Business use only**. Our data and information are intended to be used only for Firm business.
- **Be mindful of your surroundings.** Use caution when reading or displaying Confidential and Proprietary information in any location where others can see the information. Never leave Firm

devices or printed materials containing Confidential and Proprietary Information unattended in public or unsecured locations**.**

- **Only access what you are authorized to see**. Many systems and/or data require approval on a per-user basis before access is granted.
- You may not access or attempt to access any data or systems for which you are not approved. If you inadvertently access data or systems, exit immediately and notify Technical Support.
- If you receive data, information, files, or documents containing information that you do not have a need to know or authority to receive, immediately secure it from view, then delete or shred it.
- **Expressly label Confidential and Proprietary Information**. If you create a document, spreadsheet, presentation, report, or other material containing Confidential and Proprietary Information, label it as "Confidential and Proprietary."
- **Transport or send Confidential and Proprietary Information securely**. If you must send Confidential and Proprietary Information outside of the Firm, it must be encrypted or transferred via a secure portal. Contact Enterprise Security if you need assistance in determining how to encrypt, securely transfer, or physically move Confidential and Proprietary Information.
- **Do not send Firm materials or information to personal email accounts.** This includes the use of Gmail, Yahoo, or other free or paid personal email services whether for testing or for any other kind of communications.
- **Do not send Firm materials or information to unauthorized cloud locations, peer-to-peer file sharing applications, or unauthorized storage devices.** This includes but is not limited to:
- Unauthorized non-Firm cloud storage locations, peer-to-peer file sharing applications such as Dropbox, iCloud, Google Drive, OneDrive Personal accounts, Torrents, or PDF conversion sites.
- Unauthorized non-Firm storage devices such as personal storage devices (thumb drive, USB, Bluetooth, Network Attached Storage, etc.), CDs, DVDs, Blu-Ray Discs, personal PCs, MP3 players, or mobile devices (when the mobile device is used as a storage device).
- **Third-Party Access to Firm Information.** Do not grant non-Firm employees or other third parties (e.g., personnel that do not have a kforce.com email address) access to Firm Technology Resources or information in the cloud such as SharePoint Online, OneDrive, or Microsoft Teams.
- **Do not copy copyrighted or trademarked material belonging to others or violate anyone else's intellectual property rights.**
- **Store critical business documents in Firm managed storage locations.** The Firm does not back up documents stored on your laptop or desktop hard drive**.** The same is true for your personal technology devices. Store documents important to our business on your Kforce OneDrive, SharePoint, or other Firm-provided storage locations.
- **Protect your employee badge**. If you are issued a badge by the Firm or a client, do not display it in public and do not post pictures to social media with your badge visible. Pictures on social media are a key information source for bad actors to replicate your badge.
- **Pictures.** Pictures of individuals, Firm information, Technology Resources, or facilities containing Confidential and Proprietary Information must be protected.

Password Controls

Your login credentials – your username, password, and in some cases, Multifactor Authentication (MFA) are the keys that unlock access to Firm systems and information. Strong and well-managed passwords help prevent bad actors from accessing our information.

- **Minimum password requirements.** The passwords you use to access our systems – including through mobile devices – must meet or exceed the following criteria:
- be at least 12 characters long, changed every 120 days, cannot be any of your last 8 passwords;
- be a minimum of 3 out of the following 4 character sets: 1) numbers, 2) lowercase letters, 3) uppercase letters, and 4) special characters such as !, @, #, %, ^, and &.

Do not use obvious information such as your first or last name, names of family members or pets, phone numbers, birthdays, anniversaries, obvious words, hobbies, or favorite sports teams. Doing so makes it easier for someone to guess your password.

- **Use only *your* login credentials.** Do not log in using anyone else's credentials or let anyone else log in with your credentials. You are responsible for all actions associated with your account.
- **Unique passwords.** If you are issued multiple accounts to access Firm Technology Resources, do not use the same password for any account.
- **Protect your Firm username and Password.** Protect your login credentials and all passwords used for Firm business from unauthorized disclosure to *anyone* - both inside and outside our Firm.
- Do not give them to anyone, whether inside or outside of the firm.
- Do not store them in an insecure location, such as on a sticky note, under your keyboard or in your Contacts list.
- Do not use your Kforce credentials to login to your personal applications, i.e., email, social media accounts, financial applications, etc. If any of those applications experience a data breach, Kforce applications and data are at risk.
- Do not use Firm passwords for personal accounts. Do not use the same password for both your Kforce account and your personal accounts.
- **Do not attempt to circumvent the password or the MFA entry process.** Do not use auto-login or an application's remember my password feature where it is not already applied by the Firm. Also do not hard coded passwords in scripts or software.

Firm-Provided Technology Devices

Firm-provided technology devices include, but are not limited to, desktops, laptops, tablets, and smartphones.

- **Return all Firm assets.** Upon termination of your employment, assignment, contract, or agreement, you will promptly return all Firm assets in your possession in accordance with Kforce

instructions. This includes physical documents, employee badge, office keys, and other items as applicable.

- **Protect Firm-provided technology devices.** Use password protection and physically protect the technology devices.
- Never leave your device unattended when in public.
- Do not walk away from the device if you are logged into your account. Lock or completely log off the device.
- Do not allow non-Kforce personnel, including family or friends, to use your device for any reason.
- When traveling, keep your device with your carry-on luggage – do not store it in checked luggage.
- If you need to leave your device in your vehicle, do not leave it in plain view. Lock it in the trunk or keep it out of view.
- **Use only approved and licensed hardware, software, internet, and wireless tools.** For clarity:
- do not install or download any software – including free software such as a screen saver, background, game, etc. – until and unless approved through the Non-Standard Software process. Contact Technical Support to initiate this process.
- do not install or use hardware or software tools that evaluate or compromise the security of Firm Technology Resources (for example, tools that discover passwords, decrypt encrypted files, identify security vulnerabilities, capture network traffic, etc.)
- do not use software that is not legally licensed to the Firm
- do not install personally owned software on a Firm-provided technology device, and conversely, do not install Firm software on an unauthorized personal device
- do not enable auto-update processes unless it is for Firm authorized cloud-based solutions
- do not use remote desktop software or remote desktop websites such as gotomypc.com to access Firm devices
- do not load or utilize unapproved encryption technology or algorithms
- do not connect Firm technology devices to Kforce Employee Wireless Network or Kforce Guest Wireless Network
- do not modify any Firm-provided hardware, including but not limited to updating firmware, removing a hard drive, or adding memory, these types of modifications can only be performed by authorized IT personnel

Emails, Messaging, Internet, and Network Usage

- **Do not use personal email to conduct Firm business.** When the Firm provides you an email account, it must be used to conduct Firm business. When you represent Kforce, you must use your Kforce email address.

- **Encrypt Outlook emails that contain Sensitive Personal Information or Confidential and Proprietary Information.** Use the Options / Encrypt buttons in the Email Ribbon bar to encrypt the email and control forwarding.
- **No expectation of privacy.** Internet sites and Messages accessed or sent by/through Firm Technology Resources are monitored and belong to the Firm. Associates and consultants should have no expectation of privacy in these communications or their internet use activities when using Firm Technology Resources or their own devices to access Firm systems.
- The Firm has the right, with or without cause or notice, to review, examine, archive, retrieve, restore, investigate, and delete all messages and internet usage, whether in transit or stored, and we regularly monitor site usage, system activity, and communications to ensure compliance with our policies.
- **Kforce email template.** Be sure your email template includes the official Firm confidentiality notice at the bottom of the email.
- **Watch out for phishing emails. Be careful with attachments and URLs.** Use caution when you receive emails with attachments or URLs even if you know the sender. This is the primary way bad actors place malware onto our systems or compromise your credentials. You will always receive unsolicited emails and attachments, so look for common phishing indicators before opening an attachment or clicking on a URL.
- NOTE: Our Firm will not send you an email or a text asking you to enter your login credentials. Technical Support will never ask you for your password.
- **Do not send anonymous or disguised Messages.**
- **Do not use Firm Messaging, information systems, internet access, social media accounts, or any other Technology Resource to:**
- defame, libel, slander, or harass any individual or the Firm
- violate any local, state, or federal laws nor Firm policies that seek to prevent unlawful harassment or discrimination
- distribute or access pornographic material, chain letters, spam, malware, or any obscene, hateful, intimidating, gambling, or other objectionable materials
- download, use, distribute, or access hacking tools
- request donations or send mass mailings except as authorized by management
- **Do not add third parties to Team Distribution Lists.** This includes contractors and Kforce consultants. Team distribution lists are typically embedded in department distribution lists which are used to share Confidential and Proprietary Information or information that should only be shared internally.
- **Do not disable or by-pass the Web proxy.** It protects you from websites with malware and websites that are inappropriate for business use.
- **Be aware when using public networks and computers**.
- If you use a Kforce device on a public network for Firm business, use VPN for a secure connection.
- If using a personal device for Firm business, be sure the browser connection is secure (https).
- If you must use a public computer for Firm business, be sure to log out when you are finished.

- **Do not connect a personal technology device to the Kforce Firm Network.** Only Firm-provided technology devices are authorized to connect to the Kforce Production Network. Employees may connect their personal devices to the Kforce Employee Wireless Network.
- **Guests and business partners visiting a Kforce facility.** Guests and business partners may only connect their devices to the Kforce Guest Wireless Network, if available. Guests and business

  partners should never connect to the Kforce Employee Wireless Network, Kforce Firm Network, or any physical network ports.
- **Do not install a personal wireless access point, an unauthorized modem, or VPN connection on any of the Kforce Networks**. Only authorized IT personnel are permitted to do so.
- **While connected to any one of the Kforce Networks, you may not simultaneously connect to any other network .**
- **Use only authorized methods for remotely accessing our networks or systems.** Only use Firmauthorized methods and technology devices for remote access.

Mobile Devices

No one is required to use a personal device for work purposes. However, you may choose to use MultiFactor Authentication (MFA) on your personal device.

For associates, personal mobile devices may be allowed access to Firm systems and information via authorized methods such as mobile applications like Concur, CRM, or Mobile Application Management (MAM) services which provide access to multiple applications. The MAM services enforce specific security configurations for Kforce-approved applications on your mobile device, like password protection and session time out.

If you choose to use a personal device for work purposes, you agree to follow this policy, and you also agree that:

- if you are a consultant, you are not permitted to store, transmit, or process client data using your device unless specifically and expressly authorized to do so by your customer/client and Kforce
- you are responsible for securing your device if it contains or accesses Firm or client information by using password protection, session timeouts and by safely storing it
- you are fully responsible for supporting your own device and you are responsible for the cost, care, maintenance, or usage charges for your device unless you meet the criteria established by the Firm for reimbursement
- you will not use jail-broken or rooted mobile devices to access Firm or client systems or data, as this bypasses critical security controls
- you will stay current on updates applicable to your devices' security and operating systems
- you will not allow any unauthorized users or family members to access any Firm or client information through your mobile device

- you will immediately notify Technical Support if your device is lost, stolen, or otherwise compromised
- you will remove all Kforce applications and data prior to upgrading, selling, or transferring your mobile device to another individual or business
- you will promptly remove or return all Firm and client information on your personal technology device when your employment with the Firm or engagement with the client ends. The Firm reserves the right to remotely wipe all Firm data from your personal device at any time without notice
- you will surrender your personal technology device for inspection/information extraction if there is a regulatory, legal, or policy need to do so, and you will fully cooperate with Firm investigations. You also agree that the Firm is not responsible if any personal data is inadvertently deleted when MAM service, Firm applications, or Firm or client data are removed from your device. In addition, you agree that the Firm is not responsible for any negative impact the MAM service may have on your personal technology device
- you agree that, if you are an hourly employee, you will record and timely report all time worked, including the time that you spend reviewing work-related communications and matters on your personal device, so that you can be paid fully and fairly for all of your working hours

To be clear, it is not our intent, and this policy should not be interpreted, in any way to prohibit lawful personal conduct or use of your own devices during nonworking hours or to interfere with your rights under applicable federal, state, or local law.

Acceptable Use Agreement

By continuing to work for Kforce, you acknowledge and agree that you have read, understood, and will follow this policy. You also agree to do your part to stay informed about and adhere to updates to this policy and agree to take all required information security training. You will also be asked to electronically acknowledge your agreement to this policy from time to time.

Policy Name:	Timekeeping and Fair Pay Practices	**Revised:**	08/17/2018
Applicable to:	All Kforce Non-Exempt Employees, Consultants, Companies & Locations	**Customer Solutions Center:**	1-888-435-7957, option 1, CustomerSolutionsCenter@kforce.com

We value and respect all of our associates and consultants, and want to ensure everyone is fairly compensated for all time worked. This policy outlines the timekeeping requirements needed to help us honor this commitment.

Time Records. Kforce wants you to get paid for all hours you work, so accurate and honest timekeeping is required. All associates must accurately and completely record all hours worked in MyTE or in their applicable time sheets or timekeeping systems. Time records must be approved by your supervisor and submitted to Payroll by the required deadline so that we can ensure you are timely paid for all hours worked. At no time are you authorized to perform any work without recording that time in the applicable timekeeping system (i.e. no working "off the clock"). You should review your payroll statement each week. If you believe your paycheck is inaccurate for any reason (such as inaccurate hours worked or incorrect rate of pay), please bring that to the attention of Human Resources as soon as possible.

Please understand that altering, falsifying or tampering with timekeeping records, recording hours not worked, working hours not recorded (working "off the clock"), having someone else record your time or recording another employee's time can result in discipline, up to and including termination, as we consider this as a violation of our Core Values and Commitment to Integrity. No manager, supervisor or client should encourage you to avoid reporting time worked, and associates receiving any such suggestion should report the circumstances immediately. If you are encouraged at any time to report your hours worked inaccurately, please use the Open Door Policy to report it. Our policies protect you from retaliation for making these kinds of reports.

Overtime. Sometimes urgent deadlines or large projects require overtime to complete assignments on time. If you believe it is necessary to work overtime to complete work that has been assigned to you, your supervisor may require you to get his or her approval in advance and often our clients have similar requirements applicable to consultant overtime. If you violate this policy you must still record all the time that you work, and you will be paid for the hours you work, but you could be subject to disciplinary action for violating preapproval requirements.

Unless otherwise required by applicable law, you will be entitled to one and a half times your regular rate of pay for any hours worked in a one-week period in excess of forty (40) hours. There are a few states that require overtime be paid if an employee works over 8 hours in one day. For purposes of calculating overtime, the workweek is considered to begin on Monday and end on the following Sunday unless we specify otherwise to you in writing. Paid time off, holidays, bereavement, jury duty, other leave without pay, and other leave with pay are not considered time worked when computing overtime pay.

Estimating / Rounding.

- Core Associates: When recording your time on your time sheet or in a timekeeping system, please round your time worked to the nearest tenth of an hour unless the timekeeping system requires a different increment.
- Consultants: When recording your time in MyTE or other timekeeping system, please record the exact time you work. If the timekeeping system you are using requires you to round, please consistently round your time to the smallest increment of time permitted by the system (if the

system allows time to be reported in one-tenth increments, please do so, but if the lowest increment permitted by the system is quarter-hours, please round to the nearest quarter-hour).

Leaving Early / Arriving Late. You are expected to work your regularly scheduled hours. From time to time, if there are extenuating circumstances that require you to leave early or arrive late you must get your supervisor's approval in advance.

Make-Up Time. In general, you should work your regularly scheduled hours. In some states working over eight (8) hours in one day triggers overtime. If it is necessary to make up time, you will need to get your supervisor's approval of the specific change to your work schedule (i.e. date and hours) in advance. You are not authorized to work outside of your scheduled hours without authorization from your supervisor. To the extent it is approved in advance, make-up time must be worked within the same workweek. "Comp" or "makeup" time that extends into future workweeks is strictly prohibited.

Running Department Errands. Department errands should not be done during your unpaid lunch break. See also our Meal and Break Policy. To the extent you perform work-related errands outside of the workplace, you should enter your time as "time worked" on your time sheet / MyTE as applicable. Also, please be sure to track your mileage and any expenses as appropriate so the Firm can reimburse you for your business expenses.

Travel Time for Non-Exempt Employees. Your normal commute to and from work is not compensable. Travel time between offices is compensable during normal business hours. Please track and record your hours on your time sheet / MyTE so you can be paid for all hours worked. Please remember to submit your mileage and expenses as appropriate for reimbursement.

Who Should I Call?

- If you have questions about time sheets / MyTE you should contact Time Entry
  - Core associates should contact CorpTimesheets@kforce.com; and
  - Consultants should contact CustomerSolutionsCenter@kforce.com.
- If you have wage and hour questions, contact your HR representative.
- For questions regarding classifications (non-exempt vs. exempt), contact your HR representative or our Compensation team at Compensation@Kforce.com.
- In addition, you are always welcome to use the Open Door Policy to report any concerns.

Policy Name:	Meal and Break Policy	**Revised:**	8/25/2020
Applicable to:	All Kforce Non-Exempt Employees and Consultants	**Customer Solutions Center:**	1-888-435-7957, option 1, CustomerSolutionsCenter@kforce.com

As a commitment to our Great People, Kforce provides employees and consultants with meal and rest breaks, and also fully complies with all federal, state, and local laws regarding these periods. To the extent that this policy conflicts with any meal or rest break laws, the applicable law will govern. Meal and rest breaks are intended to give non-exempt employees and consultants time to relax, refresh, eat or drink, and otherwise use the time as they wish. Work should not be performed during these periods.

Meal Breaks

If you work at least five consecutive hours in a day you are eligible (and in some states required) to take an unpaid meal break of at least 30 minutes (many managers permit unpaid breaks of an hour). Meal breaks should be scheduled in consultation with your manager and in accordance with any applicable state laws. You may leave the premises during your meal breaks, but you should record the time you begin or end your meal breaks as set forth in our Timekeeping and Pay Practices Policy. Meal breaks are not counted toward total hours worked.

During your meal breaks you must be completely relieved from duty and you must not perform any work duties. If you are required to perform any work duties while on your meal break for any reason, or if you do perform work for any reason during that time, you must have approval of your direct manager and record the time as hours worked and you will be compensated for the time spent working.

Please understand that failure to record your meal breaks accurately may result in disciplinary action, up to and including termination.

Rest Breaks

You are eligible to take a paid 10-minute rest break during each 4-hour period of work (or major fraction thereof). Employees and consultants should not clock out/in for approved 10-minute rest breaks. The rest break time begins at the time you leave your workstation and concludes when you return to your workstation.

Rest breaks are intended to provide workday relief; accordingly, they should not be taken at either the beginning or end of the workday to offset arrival and departure times. Also, rest breaks should not be combined or added to meal breaks. Your manager may require that you remain on the work premises during your rest periods. Please work with your manager to schedule your rest breaks.

Failure by a manager to authorize or permit an employee to take an allotted or required meal or rest break can result in disciplinary action, up to and including termination.

Specific Requirements for California Employees and Consultants

California has specific meal period and rest break rules. We expect our California employees and consultants to take all meal periods and rest breaks as required by California law, and we also encourage rest breaks and meal periods to be taken away from your regular work area.

Meal Periods – California Only

- Employees or consultants who work more than five (5) hours in a workday are provided an unpaid, off-duty, uninterrupted meal period of at least 30 minutes, which must begin before the end of the fifth hour of work.
- Employees or consultants, with Kforce's agreement, may waive their 30-minute unpaid meal period in writing only, when they will work six (6) hours or less in one workday. The Meal Break Waiver form should be completed by the employee or consultant prior to working their shift.
- Employees or consultants who work more than 10 hours in a workday, are provided a second, unpaid, off-duty, uninterrupted meal period of at least 30 minutes, which must begin before the end of the tenth hour of work. Employees or consultants, with Kforce's agreement, may waive their second 30-minute unpaid meal period in writing only when they will work 12 hours or less in the workday, and only if they have not waived their first meal period that day. The Meal Break Waiver form should be completed by the employee or consultant prior to working their shift.
- Meal Break Waiver forms may be obtained from your Kforce HR representative.
- Employees and consultants must be relieved of all duties during their meal periods, and meal periods must not be interrupted. In addition, meal periods may be taken away from your work area and premises. If for any reason you are not able to take your meal periods consistent with this, please notify your Kforce manager or Kforce HR representative immediately. Employees or consultants may do so without fear of retaliation, which Kforce policy prohibits.

Rest Breaks– California Only

- Employees and consultants are authorized and permitted to take one 10-minute net rest break for every four (4) hours worked (or major fraction thereof) as set forth in the chart below. The rest time is paid time.

Hours Worked	Number of rest breaks
0 -3.5	0
3.5-6.0	1
6.0-10.0	2
10.0-14.0	3
14.0-18.0	4

- Insofar as practicable, employees and consultants should take their rest breaks in the middle of each work period. If an employee or consultant works less than three and half (3 ½) hours in a workday, a rest break is not required.
- Employees and consultants must be relieved of all duties during their rest breaks, and rest

breaks must not be interrupted. In addition, rest breaks may be taken away from your work area and premises. If for any reason you are not able to take your rest breaks consistent with this, please notify your Kforce manager or your Kforce HR representative immediately. Employees or consultants may do so without fear of retaliation, which Kforce policy prohibits.

Reporting and Enforcement – California only

- As stated above, if for any reason you are not able to take your meal breaks or rest periods consistent with these requirements, please notify your Kforce manager or your Kforce HR representative immediately. You should also contact your Kforce HR representative if you have questions. You are also always welcome to use our Open Door Policy, including our third-party Integrity Hotline, to report any issues or concerns.
- If you report working during your meal period or rest break, returning to work prior to the end of your meal period or rest break (without the ability to restart a full and timely meal period or rest break after the interruption ends), being denied a meal period or rest break, or being required to delay your meal period until after the end of your fifth hour of work, then you will be paid in accordance with California law.
- Employees will be subject to discipline, up to and including termination, for violating this Meal Period and Rest Break policy.

A Note About Radios, Phones, and Other Devices – California only

- Employees are not required or encouraged to carry their radios, phones, pagers, or any other device during their meal periods or rest breaks and will not be subject to any discipline for failing to do so. If any employee voluntarily chooses to carry any such device, the employee is not required to answer or otherwise respond to any call, email, text message, instant message, page, or any other interruption during their meal period or rest break and will not be subject to any discipline for failing to do so. An employee who is interrupted during a meal period or rest break is to report that fact promptly to your Kforce manager or your Kforce HR representative so that Kforce can remedy the situation.

Specific Requirements for Colorado Employees and Consultants

Colorado has specific meal and rest periods. We expect our Colorado employees and consultants to take all meal and rest breaks as required by Colorado law, and we also encourage rest breaks and meal periods to be taken away from your regular work area.

Meal Breaks – Colorado Only

Employees or consultants who work more than five (5) consecutive hours in a workday are entitled to and expected to take a duty-free, uninterrupted meal period of at least 30 minutes to be taken (when practicable) after the first hour of work and before the last hour of work begins. Meal breaks will be unpaid; however, if for any reason your meal break is interrupted with work or you perform work during your meal break, please record the time worked in MyTE (or other applicable

timekeeping system) so you can be properly compensated for that time. If you are continually interrupted during meal breaks, or if your on-site supervisor or manager does not allow you to take a meal break in accordance with this policy, you must promptly contact your recruiter or HR representative.

Rest Breaks – Colorado Only

Employees and consultants are entitled to and expected to take a paid10-minute rest break for every four (4) hours they work (or major fraction thereof), as follows:

Work Hours	Rest Periods Required
2 or fewer	0
Over 2, and up to 6	1
Over 6, and up to 10	2
Over 10, and up to 14	3
Over 14, and up to 18	4
Over 18, and up to 22	5
Over 22	6

When practicable, rest breaks should be taken in the middle of each 4-hour period of work. Kforce encourages employees to take all allotted rest breaks. These required rest breaks are considered time worked for purposes of calculating overtime. If your on-site supervisor or manager does not allow you to take a rest break in accordance with this policy, discourages you from taking an allotted break in any manner, or if you feel your job duties workload do not allow you to take rest breaks in accordance with this policy, you must promptly contact your recruiter or HR representative. Kforce will compensate employees appropriately for any missed rest break.

Questions and Enforcement

When recording your time into MyTE (or other applicable timekeeping system), you will be asked to attest that you have taken all allotted meal and rest breaks and recorded all time worked. Kforce will rely on your submission of your timecard with this attestation. Therefore, it is very important that you notify your manager, recruiter, or HR representative immediately if for any reason you are not able to take your required meal break or rest breaks in accordance with this policy. Failure to accurately report break times, including any missed or interrupted breaks, as well as any other violations of this policy may subject employees to disciplinary action, up to and including termination. You are also always welcome to use our Open Door Policy, including our third-party Integrity Hotline, to report concerns. Kforce will not tolerate retaliation against employees who report any concerns of policy violation in good faith.

Policy Name:	Safe Work Environment Policy	**Revised:**	04/12/2021
Applicable to:	All Kforce Employees, Companies & Locations	**Alert Line & Other Important Contact Information:**	Alert Line: 813-552-3399 Risk Management: 813-552-2109 Employee Assistance Program: 833-789-9882

We are committed to providing a safe work environment. All employees, candidates, consultants, vendors and other business partners should be treated with courtesy and respect, and no one may engage in threats, bullying, intimidation or any other acts or threats of violence. In addition, we are committed to supporting our employees and consultants who may face situations where their safety is endangered; such as when they or their loved ones face concerns of domestic violence, suicide, or abuse.

Violence or threats of violence in the workplace are strictly prohibited. In addition, violence or threats of violence outside of the workplace that could affect someone's ability to work are prohibited by this policy. For the purposes of this policy, violence is defined as actual or potential assault, battery, intimidation, threats, stalking, bullying, destruction of property, or any similar act that occurs while an individual is engaged in Firm business, at a Firm or client site, or while attending a Firm-sponsored event. Violence also includes the same kinds of activities outside of work if they could have an adverse effect on someone's ability to work.

When any act or threat of violence occurs, we will take immediate action. Any person who makes threats, exhibits threatening behavior, or engages in violent acts will be removed as quickly as safety permits, and may be asked to remain away from Firm or client worksites pending the outcome of an investigation. Depending on the situation, we may also suspend or terminate the affected business or employment relationship, reassign job duties, report the situation to law enforcement, criminally prosecute the persons(s) involved or take whatever other action we believe is necessary to protect our workplace.

Dangerous or illegal items of any nature such as weapons, explosives, or firearms are not permitted within any Firm or client office without express approval of Kforce Security Services. Individuals with authorized permits or licenses may have firearms or weapons in their locked vehicles in parking areas where allowed by law. Even with conceal carry permits, weapons and firearms are not permitted in Firm or client offices unless you have pre-registered and obtained written approval from Kforce Security Services. Certain locations may have more restrictive prohibitions based upon local laws or landlord leases, and we must obey the law and policies where our offices are located. In addition, consultants on assignment must abide by our client's policies regarding firearms and weapons possession.

Violations of this policy will lead to disciplinary actions up to and including immediate termination of employment and may also be referred for criminal prosecution.

Domestic Violence, Suicide and Abuse

We understand the traumatic impact that domestic violence, suicide and abuse can have in the workplace.

We work to protect our employees and consultants against domestic violence and other forms of bullying and abuse while in our workplaces, and we will make assistance available to them to help with these difficult circumstances. This assistance may include, but is not limited to, providing a discrete means of coming forward for help, resource and referral information, special workplace accommodations, work schedule adjustments, leave if necessary to obtain medical, counseling, or legal assistance, and, in

extreme cases, workplace relocation (if available). Employees or consultants who need assistance or who apply for and obtain a protective or restraining order that lists any of our offices or client locations as a protected area should notify and work with Human Resources.

Acts or threats of suicide are tragic and can have far-reaching effects on family, friends, colleagues and communities. We offer support to our employees and consultants who have experienced a suicide crisis or who are aware of suicide risks. In particular, if you become aware of another employee's intent to harm others or themselves please notify Human Resources right away. We encourage our employees and consultants to contact Human Resources or our alert line as listed below, for information on the assistance available to them.

You can also contact our Employee Assistance Program (EAP) at 833-789-9882. Participation in EAP services and any recommended treatment is confidential.

Reporting and Requests for Help or Assistance

If you witness or hear of a potential act of workplace violence, a domestic violence matter, a threat of suicide or serious self-harm, or other conduct covered by this policy please call 911 immediately if it is an emergency. If the situation is not an emergency, or if you've already called 911, please then call our alert line at 813-552-3399. We strictly prohibit retaliation against anyone raising a concern of violence in good faith. Please understand that failure to report violations of this policy that you experience or witness could result in termination of your employment or business relationship with Kforce.

Keep Us Informed

As a part of our efforts to maintain safe work environments for all of our associates, consultants, and clients we need to be aware of any criminal activity that could impact our workplaces. Accordingly, all associates and consultants must immediately report all criminal arrests and convictions (other than routine speeding or other non-alcohol related traffic violations) to a Human Resources Business Partner. Reporting a matter does not mean we will take adverse action involving your employment. Rather, we evaluate all such reports on a case-by-case basis to determine whether the offense is job-related or jeopardizes workplace safety.

Policy Name:	Statement of Availability Policy	**Revised:**	10/01/2013
Applicable to:	All Kforce Employees, Companies & Locations	**Customer Solutions Center:**	1-888-435-7957, option 1, CustomerSolutionsCenter@kforce.com

Kforce requires all consultants to adhere to the following policy when an assignment with Kforce is complete:

- The consultant must contact their recruiter at Kforce the same day an assignment ends and weekly thereafter to advise of their availability as part of the consultant's attempts to secure employment.
- Failure to contact your recruiter at Kforce for reassignment or refusal of an assignment may result in the loss of unemployment benefits under your state unemployment insurance code.
- Kforce will notify your state unemployment agency if one of the following occurs:

    1. Failure to contact your Kforce recruiter for reassignment the same day an assignment ends.
    2. Refuses a reasonable assignment or offer of employment.
    3. Fails to respond to the employer's mail, e-mail or telephone calls regarding reassignment.
    4. Fails to notify Kforce recruiter of your work availability on a weekly basis.

If you fail to follow terms stated above at any time, Kforce will assume that the consultant is not available for assignment and will so advise the state agency inquiring about your employment status.

Policy Name:	Internal Privacy Policy	**Revised**:	August 26, 2021
Applicable to:	All Kforce Employees, Consultants, Companies & Locations	**Customer Solutions Center:**	1-888-435-7957, option 1, CustomerSolutionsCenter@kforce.com

Purpose

Kforce Inc. (the **Firm**) has adopted this Policy to govern the treatment of all Personal Information. The loss of Personal Information can result in substantial harm to individuals, including embarrassment, inconvenience, and fraudulent use of the information. Protecting the confidentiality and integrity of Personal Information is a critical responsibility that must be taken seriously at all times. Compliance with this Policy is mandatory.

The purpose of the Policy is to:

- Define Personal Information and Sensitive Personal Information.
- Establish general principles for protecting Personal Information.
- Assign accountability for protection of Personal Information.

Scope

This Policy applies to all Firm employees, associates, contractors and consultants (**Personnel**), including any subcontractors or third-party provider of services to the Firm (**Third-Party Service Provider**) who have access to Personal Information the Firm has collected or otherwise has in its possession. This Policy applies to all Personal Information collected, maintained, transmitted, stored, retained, or otherwise used by the Firm regardless of the media on which that information is stored and whether relating to candidates, consultants, employees, independent contractors, clients, or any other person.

Definitions

- **Personal Information** is inclusive of all PII, PHI and Sensitive Personal Information. It also means any information that can be reasonably linked to any one person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, physical addresses, email addresses, telephone numbers, other identifying numbers, any financial identifiers, biometric information, internet activity, geolocation data, and personal trends. (See Appendix for details)
- **Data Subject** means the person about whom Personal Information is collected.
- **Personally Identifiable Information or PII** is information that can be used to identify, contact, or trace a unique living individual. PII can be electronic or in paper form. Although the definition of PII varies state-to-state, the typical definition is:

  The first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to the individual:

  - Date of birth (month, day, and year) ○ Social Security Number
  - Driver's license number, federal or state-issued identification card number ○ Financial account, credit, or debit card number (with or without any required security

code, access code, personal identification number (PIN), or password) that would permit access to an individual's financial account

- **Protected Health Information or PHI** means any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.
- **Sensitive Personal Information** is inclusive of all PII or PHI and further entails:

  (1) Personal Information that reveals (A) social security, driver's license, state identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) precise geolocation; (D) racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of mail, email and text messages, unless the business is the intended recipient of the communication; or (F) genetic data; or

  (2)(A) the processing of biometric information for the purpose of uniquely identifying an individual; (B) Personal Information collected and analyzed concerning an individual's health; or (C) Personal Information collected and analyzed concerning an individual's sex life or sexual orientation.

  Sensitive Personal Information that is "publicly available" shall not be considered Sensitive Personal Information or Personal Information.
- **Privacy Incident** is any event that has resulted in (or could result in) unauthorized use or disclosure of Personal Information where persons other than authorized Personnel have access (or potential access) to Personal Information or use it for an unauthorized purpose. **Data Privacy Principles**

The Data Privacy Program is built upon the following Data Privacy Principles that guide what Kforce strives for as it relates to the Core Values in the Commitment to Integrity and also what is operationally reasonable and practicable:

- Personal Information will be processed* in a lawful, fair, and transparent manner.
- Personal Information will be collected for necessary and legitimate purposes.
- Personal Information will be used for the purpose for which it was collected or as permitted under the Firm's Privacy Policy and applicable law.
- Data Subjects will be informed of the types of Personal Information collected about them and how it will be used.
- Personal Information will be kept accurate and up to date.
- Personal Information will be destroyed when it is no longer needed.
- Sensitive Personal Information will be de-identified where possible, and only reidentified for a legitimate business purpose.
- Personal Information will be protected from unauthorized access, accidental loss, damage or destruction.
- Kforce will fulfill its regulatory requirements.
- Kforce will fulfill its contractual requirements.
- Kforce and all Personnel will process* Personal Information with appropriate measures in place to assure all Privacy Principles are adhered to.

** Processing includes the collection, organization, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of Personal Information.*

Using, Handling, and Retaining Personal Information

***Notice and Collection*.** It is Firm policy that whenever it collects Personal Information for any purpose, including for human resources or employment purposes, it must inform the Data Subject of how it will use, process, disclose, protect, and retain that Personal Information by presenting a privacy policy or privacy notice to the individual at the time the individual provides the Personal Information. Personnel may only collect Personal Information in compliance with applicable Firm policies, notices, and Data Subject consent, and the Personal Information collected must be limited to that which is reasonably necessary to accomplish the Firm's legitimate business purposes or as necessary to comply with law.

***Access, Use, and Sharing of Personal Information*.** Personnel may only access Personal Information when the information relates to and is necessary to perform their job duties. Personnel may not access Personal Information for any reason unrelated to their job duties. Personnel may not use Personal Information in a way that is incompatible with the notice given to the Data Subject at the time the information was collected. Personnel may only share Personal Information with another Firm employee, agent, or representative if the recipient has a job-related need to know the information. Personal Information may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the Personal Information complies with the privacy notice provided to the Data Subject. In addition, whenever Personal Information is entrusted to a Third-Party Service Provider, proper management and supervision over the outside party's handling of that Personal Information is required. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with privacy@kforce.com.

Sensitive Personal Information if lost, compromised, accessed, or improperly disclosed could result in harm, embarrassment, inconvenience, or unfairness to an individual and therefore is subject to heightened protections.

In most jurisdictions, the law will provide for the types of information that are subject to heightened protection. If you have any questions about whether any Personal Information qualifies as Sensitive Personal Information, you should contact privacy@kforce.com.

***Accuracy*.** Personnel must collect, maintain, and use Personal Information that is accurate, complete, and relevant to the purposes for which it was collected.

***Security*.** Personnel are responsible for protecting Personal Information. The Firm and its clients have set forth technical, administrative, and physical safeguards for the protection of Personal Information. All Personnel must follow the security procedures set out by the Firm and/or its clients at all times. All Personnel must exercise particular care in protecting Sensitive Personal Information from loss, unauthorized access, and unauthorized disclosure.

***Data Subject's Rights*.** Individuals have rights when it comes to how their Personal Information is handled. These rights may vary depending on the applicable jurisdiction, but may include for example:

- The right to know what Personal Information the Firm maintains about the individual and/or with whom the Firm has shared the Personal Information.
- The right to access and/or correct the Personal Information.
- A right to delete the Personal Information.

- A right to opt-out of Personal Information sales.
- A right to opt-out of using Personal Information for marketing purposes.

The Firm must comply with applicable laws regarding the rights of Data Subjects. If you are unsure of the applicable legal requirements, or if you receive a request or complaint from a Data Subject regarding the handling of his or her Personal Information, please contact privacy@kforce.com.

If you receive a request from a Data Subject regarding their Data Subject Rights, please redirect them to the Privacy Rights webform on www.kforce.com or to privacy@kforce.com.

***Retention and Disposal*.** Personnel should keep Personal Information only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. Personnel must follow the applicable records retention schedules and policies and destroy any media containing Personal Information in accordance with the Records Retention Policy.

Training

Firm Personnel will be required to complete training on the protection, handling and integrity of Personal Information upon hire and periodically, as needed.

Monitoring Compliance and Enforcement

The Privacy team is responsible for administering and overseeing implementation of this Policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect Personal Information, has been or is being violated, please contact privacy@kforce.com. The Firm will conduct periodic reviews and audits to assess compliance with this Policy.

Reporting a Privacy Incident

If you know or suspect that a Privacy Incident has occurred, do not attempt to investigate the matter yourself. Immediately contact privacy@kforce.com. and this will initiate the Privacy Incident Response Plan. You must preserve and keep confidential all evidence and information relating to the potential Privacy Incident, and you must cooperate with Privacy team and comply with all directions and requests communicated by them in responding to the Privacy Incident

Policy Compliance

Personnel who violate this Policy and any related guidelines, operating procedures, or processes designed to protect Personal Information may be subject to discipline up to and including termination of employment.

Related Policies

Other Firm policies also apply to the collection, use, storage, protection, and handling of Personal Information and may be relevant to implementing this Policy. You should familiarize yourself with these policies, including:

- Acceptable Use Policy
- PII Handling and Incident Breach Policy (Note: only applicable to Personnel with access to Kforce managed PII.)
- Records Retention Policy (Note: applicable only to Personnel with access to Kforce Records as defined in the Records Retention Policy.)

Disclaimer of Restrictions on Employees' Rights

This Policy is not intended to restrict communications or actions protected or required by state or federal law.

Amendment and Revision

This Policy may be revised from time to time.

Privacy Agreement

By continuing to work for Kforce, you acknowledge and agree that you have read, understood, and will follow this Policy, which may be updated from time to time. You also agree to do your part to stay informed about and adhere to updates to this Policy and agree to complete all required privacy-related training. You may also be asked to electronically acknowledge your agreement to adhere to this policy from time to time.