VSP Vision Standard Workforce Policies

Contents

Definitions:

- **Contingent Worker or Service Provider** – the temporary worker assigned to perform services at VSP Global® (VSP).
- **On-Site Supervisor** – the on-site vendor management representative(s), VOLT.
- **Your Employer**- the contingent worker's or service provider's employer that placed them on assignment at VSP.

I. Introduction

Welcome to VSP Global®, a complementary group of leading companies, working together to meet and exceed the needs of eyecare professionals, clients, and more than 60 million members. Combining the strength and expertise of each of these companies, VSP Global® provides benefits, services, products, and solutions that are unparalleled in the optical industry.

The Standards of Conduct for Contingent Workforce or Service Providers describes the standards and rules that as a Contingent Worker or Service Provider for the VSP Global® companies' team, you will be responsible for performing services to our standards. Below are the policies and guidelines to meet those standards.

Note: If you have any questions or concerns regarding these policies, please speak to your onsite supervisor or your employer.

II. Anti-Harassment Policy

VSP Global® (VSP) is committed to providing a workplace free of unlawful harassment. Harassment of any Contingent Worker, Service Provider or Contingent Workers or Service Providers because of race, color, national origin, ancestry, sex (including pregnancy, childbirth and medical conditions related to pregnancy or childbirth), religious creed, religion, age (for persons 40 and older), disability (mental or physical, including HIV and AIDS), military and veteran status, medical condition (cancer and genetic characteristics), marital status, familial status* , sexual orientation, gender, gender identity and expression, genetic information, denial of Family and Medical Care Leave, or any other protected status under applicable federal, state or local law is considered an act of misconduct and appropriate disciplinary action will be taken against any Contingent Worker, Service Provider or Contingent Workers or Service Providers who violates this policy. While VSP supervisors and managers are responsible for implementing and monitoring compliance with this policy, all Contingent Workers and Service Providers assigned to VSP Global® share in the responsibility to report instances of harassment that they observe or of which they have knowledge. This Policy applies to all Contingent Workers and Service Providers.

Harassment is defined as unwelcome or unsolicited verbal, physical, or sexual conduct that:

- is made a term or condition of employment or
- is severe and pervasive and creates an intimidating, hostile or offensive working environment

Examples of what may be considered harassment, depending on the facts and circumstances, include:

- **Verbal and Visual Harassment** - Derogatory or vulgar comments made to any Contingent Worker or Service Provider because of their race, color, national origin, ancestry, sex (including pregnancy, childbirth and medical

conditions related to pregnancy or childbirth), religious creed, religion, age (for persons 40 and older), disability (mental or physical, including HIV and AIDS), veteran status, medical condition (cancer and genetic characteristics), marital status, sexual orientation, gender, gender identity and expression, genetic information, denial of Family and Medical Care Leave, or distribution of written or graphic material to the same effect

- **Physical Harassment** - Touching, hitting, pushing or other aggressive physical conduct or threats to take such action
- **Sexual Harassment** - Unwelcome or unsolicited sexual advances, demands for sexual favors, or other verbal or physical conduct such as uninvited touching of a sexual nature or sexually related comments

III. Harassment Complaint Procedures

Any Contingent Worker or Service Provider who believes he or she has been subjected to harassment is encouraged to make it clear to the offender that such behavior is offensive to them, and report the situation to your immediate on-site supervisor, your employer, or the Human Resources Business Partner assigned to the area in which the Service Provider is providing services. Any member of management receiving a harassment complaint or who becomes aware of possible unlawful harassment shall promptly contact the Human Resources Department to report the complaint for investigation. If a complaint involves a member of management, the complaint should be brought directly to Human Resources management. Harassment by Contingent Workers or Service Providers or Contingent Workers or Service Providers (i.e., Contingent Workforce, Service Providers, contractors, visitors to VSP, etc.) will not be tolerated and should be reported immediately to management. All complaints are handled in a timely and confidential manner to the extent permitted by law. Information concerning a complaint will not be released by VSP to third parties or to anyone within the Company who is not involved with the investigation

- Investigation of a complaint will normally include conferring with the parties involved and any named or apparent witnesses. Contingent Workers or Service Providers shall be provided an impartial and due Process. All Contingent Workers or Service Providers shall be protected from coercion, intimidation, retaliation, interference or discrimination for filing a complaint or assisting in an investigation.
- All complaints of harassment are investigated by the local Human Resources (HR) Department under the authority of the Chief Human Resources Officer (CHRO); all Contingent Workers or Service Providers are expected to cooperate fully in any investigation in which they may be called upon. All investigations are conducted in a fair and impartial manner by the HR and upon completion of its investigation, HR shall report its findings and determinations to the CHRO. After the investigation is concluded, HR will notify appropriate parties on a “need to know” basis of the action(s) or remedy(ies) taken to resolve the complaint.

We trust that all Contingent Workers or Service Providers assigned to VSP will continue to act responsibly to establish and maintain a pleasant working environment free of harassment, discrimination, and retaliation. VSP encourages any Contingent Worker or Service Provider to raise questions you may have regarding harassment, discrimination, retaliation or equal employment opportunity with your onsite supervisor or your employer.

*Protected status for age for New York Contingent Workers or Service Providers is 18 years of age or older. Familial status protection applies to New York Contingent Workers or Service Providers.

* Protected status for race includes protective hair styles and hair textures associated with race. Examples of protective hair styles and hair textures include braids (with extensions or adornments), locks, twists, tight coils or curls, cornrows, Bantu knots, afros, headwraps, wigs, and weaves.

** In California protected status for sex includes reproductive health decision making. This includes, but is not limited to, a decision to use or access a particular drug, device, product, or medical service for reproductive health.

IV. Code of Conduct Policy

The true foundation of VSP Global® (VSP) has always been its commitment to provide the highest quality eyecare and eyewear service to our members, customers, and vendors. As part of this service, we strive to ensure an ethical approach to VSP's delivery and management of all its lines of business. To that end, we strive to demonstrate that we act with absolute integrity in everything that involves or impacts our work at VSP.

This Code of Conduct sets forth VSP's guiding corporate principles that our work is performed in an ethical and legal manner. These obligations apply to our relationships with members, doctors, clients, independent contractors, vendors, regulators, consultants, Contingent Workers, Service Providers and one another. The Code's emphasis is on our shared global values, which guide and dictate the appropriate conduct while performing services for VSP. It is also a key component of our overall Corporate Ethics and Compliance Program.

The Code is intended to be a statement that is detailed, yet easily understood. In some instances, the Code deals fully with the subject matter covered. In many cases, however, the subject discussed is complex with references to additional policies or procedures or discussion with those who are directly involved or have direct responsibility may be necessary.

As a global Company, we are committed to those ideals which are reflected in our Mission, Vision and Values Statement, this Code, and our policies and procedures. VSP is also committed to abiding by all applicable laws, statutes and regulations where we do business. We are equally committed to assuring that our actions consistently reflect our words. In this spirit, we expect all of our Contingent Workers or Service Providers' actions to reflect the high standards set forth in the Code..

No code of conduct can substitute for your own internal sense of fairness, honesty, and integrity. Thus, in your daily life and work, if you encounter a situation or are considering a course of action which may be technically within the guidelines of the Code of Conduct, but you are concerned that the contemplated action simply "does not feel right," please discuss the situation with any of the resources listed below.

Any questions regarding this Code or a situation that you believe may violate its provisions, immediately contact your onsite supervisor, your employer, another member of management, Human Resources, or VSP's Corporate Ethics and Compliance Officer, Dan Schauer. You may also call the Ethics & Compliance Line at 877.349.7494. You have our personal assurance there will be no retribution for asking questions or raising concerns about the Code or for reporting possible improper conduct. The Ethics & Compliance Hotline facilitates anonymous reporting for any caller who wishes to remain anonymous.

Please thoroughly review this Code and all associated Company policies and procedures. Your adherence to the spirit and intent of VSP's guiding principles and policies is absolutely critical to VSP's success and future.

V. Confidential Information Policy

As a Contingent Worker or Service Provider assigned to VSP, you may have access to information of a confidential,

proprietary, technological, and/or secret nature ("Confidential Information"), which is or may be related to VSP's business, business development, research, or its customers. You must hold such information in strict confidence and not disclose or furnish at any time, directly or indirectly, to any other person, firm, agency, corporation, client, business, or enterprise, except as required by business necessity and with appropriate written authorization to disclose. This Confidential Information includes, but is not limited to, any portion or phase of:

- VSP products
- Business; business or marketing plans and strategies
- Business matters or opportunities or offerings
- Information, records, writing, correspondence, data and databases
- Financial information
- Customer, vendor or supplier lists
- Provider or patient names, addresses, and/or telephone numbers
- Patient Health Information (PHI) such as patient name(s), address(es), telephone number(s), medical records and claims information related to patient
- Novel processes and procedures
- Price lists
- Ratings applications - software or database applications used in whole or in part to calculate rates for new or existing customers
- Software (object and/or source code), and software and equipment documentation including flowcharts
- Underwriting rates and data
- Advertising and promotional ideas and strategies
- Formulas, patterns, devices, processes
- Other information which has not been published or disseminated, or otherwise become a matter of public knowledge

VI. Collection of Biometric Information Policy

VSP and its vendors collect biometric information including but not limited to fingerprints, facial recognition, and body temperature "Biometric Information"

VSP and its vendors use:

1. Your fingerprints to clock-in and clock-out for work, to accurately record the hours you work, and to process payroll;
2. Facial recognition and body temperature for its health and safety protocols (i.e., COVID-19); and
3. Facial recognition to access devices.

VSP will not sell, lease, trade, or otherwise profit from a Contingent Workers or Service Providers' Biometric Information.

Your Biometric Information will be collected and stored during the duration of your employment. When a Contingent Workers or Service Providers ends his or her employment with VSP, moves to a position that does not require Biometric Information, or if VSP discontinues collecting or using vendors that collect Biometric

Information, VSP will instruct its vendors to delete your Biometric Information. VSP and its vendors will store, transmit, and protect from disclosure all biometric identifiers and Biometric Information using a reasonable standard of care.

VII. Business Collateral

In an effort to protect VSP's Confidential Information from being disclosed, duplicated, and/or infringed upon by any unauthorized source, each line of business is responsible for designating business related information or data with the appropriate level classification. The classification options include Public, Proprietary (External or Internal), or Confidential.

Note: If a classification is not specified, there is the expectation that the information will be treated as Confidential Information

General Handling Requirements

Confidential Information is available to Contingent Workers or Service Providers assigned to VSP in many forms, including hardcopy documents, screen displays, electronic media, e-mail, discs, flash drives, PC/hard drives, servers/shared drives, databases, etc. When handling any Confidential Information, Contingent Workers or Service Providers assigned to VSP must adhere to the basic standards described below. Exceptions to these standards require approval from the security officer, privacy officer and/or line of business president.

The basic standards for Confidential Information:

- Do not leave printed or electronic media unattended.
- Lock materials in your desk or a cabinet when you leave your work area.
- Retrieve material immediately or use secure-print or printer-mailbox function when printing material.
- Immediately shred or discard printed material in designated secure bins located in your department.
- Remove or neutralize the magnetic field of unneeded discs before discarding.
- Encrypt e-mails that are to be sent beyond the VSP firewall, i.e., e-mails to customers.
- Don't create databases containing confidential information or data without proper approval from management.
- Delete confidential information downloaded to spreadsheets or files for ad hoc analysis after using.
- Don't leave computer screens unattended when displaying Confidential Information.
- If you need to step away from your computer, use the ctrl+alt+del function to lock your PC.
- All paper that contains Confidential Information of any kind is to be disposed of only in locked Confidential Document bins. To prevent accidental exposure of Confidential Information, no paper that contains Confidential Information is to be disposed of in the garbage or any other recycling bin.

Additional, highly recommended standards:

- Use standard templates for internal and external reports.
- Whenever feasible, use watermarks to clearly identify confidential material.

Information Confidentiality Classification Matrix for Service Provider

Note: “VSP” includes all VSP companies

	Public	Proprietary External	Proprietary Internal	Confidential
Description	Not sensitive; available to anyone	VSP owned; requires prior authorization for release outside of the Company	VSP owned; not to be disclosed or used outside of VSP	VSP owned; not to be disclosed or used beyond select internal or external audiences
Impact of Unauthorized Disclosure	Disclosure, use, or destruction of public information or data should have no adverse impacts on the organization or carry any liability	May adversely impact the organization; could undermine the confidence in and reputation of the organization	May seriously impact the organization; could jeopardize the organization’s competitive edge; could undermine the confidence in, and reputation of, the organization	Would severely impact the entire system, individual persons, and the public; incur financial or legal liabilities; damage confidence in, and impair the reputation of, the organization
Possible Examples	vsp.com homepage content; readily available news and information posted on Globalview and vsp.com	Product offerings; Contingent Workers or Service Providers info for confidential surveys conducted by outside entities; Provider Reference Manual; underwriting rates; internal phone number listings; audited financial reports	Contingent Workers or Service Providers login IDs; VSP’s third-party partner information; organization charts; Sales411 content; competitive data; doctor fees	Protected health information; doctor IDs; Contingent Workers or Service Providers personal information, e.g., SSN and payroll; client billing information; unaudited financial statements; budget-to- actual reports; Board minutes
Access	All	Available to Contingent Workers or Service Providers and approved Contingent Workers or Service Providers; requires prior authorization prior to disclosure outside of VSP	Available to Contingent Workers or Service Providers only; not for disclosure or use outside of VSP	Available to select Contingent Workers or Service Providers and authorized Contingent Workers or Service Providers with a nondisclosure agreement, granted on a need-to-know basis; an access list must be maintained
Handling	N/A	Same as Confidential, plus disclosure outside of VSP requires prior approval of division Vice President	Same as Confidential, plus do not disclose outside of VSP	Use secure-print or printer-mailbox function when printing; lock printed materials, discs, CDs, and DVDs in desk or cabinet when leaving work space; shred unneeded or unused printed material or place in marked secure waste bin; logout or lock computer screen when leaving desk; use encryption, e.g., Tumbleweed software, when e-mailing external information; remove or neutralize the magnetic field of discs before discarding; don’t create databases containing confidential information or data without domain-owner approval; use standard templates and watermarks for printed material whenever possible

External Surveys

Periodically, VSP receives external surveys requesting details of Company business, business operations, plans and/or products, or VSP employment practices. As a general practice, we do not participate, and Contingent Workers or Service Providers assigned to VSP are not authorized to respond to or directly initiate such external surveys.

You are not permitted to discuss any Company business with persons outside of the Company and refer all such inquiries to the appropriate line of business president. If a telephone caller has an unusual request or appears very curious about the Company's affairs, refer the call to your onsite supervisor immediately.

Unauthorized dissemination of the foregoing information to Contingent Workers or Service Providers, Contingent Workers or Service Providers, Contingent Workers or Service Providers assigned to VSP or Contingent Workers or Service Providers assigned to VSPwill cause grievous and irreparable injury to VSP, and any remedy which VSP may have for any breach thereof would be inadequate. Therefore, in addition to any other available remedies at law, VSP shall be entitled to injunctive relief without bond in a court of competent jurisdiction restraining that Contingent Workers or Service Providers assigned to VSP from violating any provisions of this policy. Contingent Workers or Service Providers assigned to VSP shall indemnify VSP against any and all liability, damages, and loss, including attorneys' fees, expert witness fees, and court costs arising out of Contingent Workers or Service Providers assigned to VSP's breach. Further, unauthorized duplication or distribution of any rating applications will be considered theft of VSP's trade secrets and a violation of state and federal copyright laws.

VII. Conflict of Interest Policy

VSP Global® (VSP) Contingent Workers or Service Providers assigned to VSP are expected to devote their best efforts and attention to the performance of their job responsibilities. Contingent Workers or Service Providers assigned to VSP are expected to use good judgment, adhere to high ethical standards, and avoid situations that create an actual, potential or perceived conflict between the Contingent Workers or Service Provider's personal interests and the interests of VSP.

A conflict of interest may arise if your outside activities or personal interests influence or appear to influence your ability to make objective decisions in the course of your job responsibilities. A conflict of interest may also arise if the demands of those outside activities/personal interests hinder or distract you from the performance of your assignment or cause you to use Company resources for purposes that are not VSP business related.

Both the fact and the appearance of conflict of interest should be avoided. Some of the more common conflicts include, but are not limited to, the following:

- Competing with VSP in any way
- Rendering service or providing a benefit (with or without compensation) as Contingent Workers or Service Providers assigned to VSP to any person, firm or corporation competing, dealing or seeking to deal with VSP
- Having ownership (direct or indirect) in any company or organization doing business with VSP

If a Contingent Workers or Service Providers assigned to VSP, or someone with whom a Contingent Workers or Service Providers assigned to VSP has a close relationship (i.e., a family member or close companion), is involved in any of the foregoing activities, the Contingent Workers or Service Providers assigned to VSP must disclose this fact in writing to your onsite supervisor or your employer. VSP reserves the right not to enter into any agreement where there is an actual, potential, or perceived conflict of interest. A Contingent Workers or Service Providers assigned to VSP may be

transferred or his/her services terminated if a conflict of interest cannot be resolved to VSP's satisfaction.

If you as a Contingent Workers or Service Providers assigned to VSP are unsure as to whether a certain transaction, activity or relationship constitutes a conflict of interest, consult with your onsite supervisor or your employer for clarification. He or she will refer questionable issues to VSP's Legal department for a final decision.

Other Employment

To avoid any conflict of interest, you must disclose to your onsite supervisor any other employment or assignments you may have. VSP will hold all Contingent Workers or Service Providers assigned to VSP to normal performance standards and scheduling requirements regardless of their activities outside VSP.

VIII. Dress Standards Policy

VSP Global® (VSP) defines its dress standard as "business casual." However, you may maintain traditional business attire for yourself. While we understand "business casual" and "traditional business" are subject to interpretation, the objective is to maintain a **neat, well-groomed** appearance.

The line of business may create specific guidelines for those engaged in work during normal business hours, where the dress standard is not practical or does not meet business needs.

The spectrum of business casual wear is broad, but not all casual attire is appropriate for our work environment. You should always dress appropriately for your assignment that day. In all cases, use your best judgment in choosing your attire. This policy is not intended to be all-inclusive.

VSP does provide dress standard accommodation where appropriate for medical, religious and/or cultural reasons.

Enforcement

The on-site supervisor/managers will counsel Contingent Workers or Service Providers assigned to VSP who come to work in attire that is inappropriate. Flagrant or repeated disregard may result in a Contingent Workers or Service Provider's assignment being terminated. Examples of inappropriate attire include, but are not limited to: athletic wear, transparent or revealing clothing, bare torso/midriffs, overly distressed clothing, t-shirts or hats with distracting or offensive slogans, and offensive tattoos. Flagrant disregard may result in a Contingent Workers or Service Providers being sent home without pay, which will be considered an unscheduled absence (occurrence). Continued disregard may result in disciplinary action.

LOB Exception

All Contingent Workers or Service Providers at the Marchon Distribution Center and the VSPOne Labs must wear closed-toe shoes with acceptable rubber treads. Contingent Workers or Service Providers working on equipment (hi-lo's, boxing machines, etc.) are required to wear the appropriate Personal Protective Equipment (PPE).

VSPOne Labs

Contingent Workers or Service Providers who operate machinery should not wear loose-fitting clothing, jewelry, or other items that could become entangled in machinery. Hair longer than shoulder length should be worn under a cap or otherwise

contained to prevent entanglement in moving machinery. Lab management may require specific PPE or clothing dependent on job duties as outlined in Lab Personal Protective Equipment Assessments.

VSPOne Lab Management may enforce a more professional dress requirement at locations where there are frequent customer tours. Contingent Workers or Service Providers should consult their on-site supervisor or employer for the established criteria at their assigned lab.

IX. Drug-Free Workplace Policy

VSP Global® (VSP) is committed to providing and maintaining a safe and secure environment for its Contingent Workers or Service Providers, Contingent Workers or Service Providers, customers, and guests. Contingent Workers or Service Provider who use drugs and/or alcohol may pose serious safety and health risks to themselves, their co-workers, and our customers. Such use also places company products, services, property and operations at risk.

VSP will take reasonable measures to maintain a work environment that is free of substance use, provides a safe and secure workplace for Contingent Workers or Service Providers, maintains the quality and integrity of VSP products and services, and preserves the Company's reputation in the communities in which the Company operates. To that end, VSP administers a comprehensive Drug-Free Workplace Policy, whereby any Contingent Workers or Service Provider using or possessing illegal drugs or other illegal substances on company premises or while conducting company business will have their services terminated immediately. Alcohol use on VSP premises and/or during scheduled work hours, including meal periods and breaks, will also be grounds for termination of service.

Contingent Workers or Service Providers who must take a prescription drug that causes adverse side effects (for example, drowsiness, or impaired reflexes/reaction time) should inform their onsite supervisor that they are using such medication at the advice of a physician. Such Contingent Workers or Service Providers are responsible for informing their onsite supervisor of the drug's possible effects on performance and the expected duration of use. If a Contingent Workers or Service Provider is using a drug that could cause production or safety problems, the onsite supervisor may grant the Contingent Workers or Service Provider sick leave or temporarily assign the Contingent Workers or Service Provider different duties if available.

VSP's drug-free workplace policy includes a prohibition on medical marijuana, in conformance with federal laws.

If you are experiencing problems with alcohol or drugs, please contact your onsite supervisor or your employer. All such discussions will be strictly confidential.

Definitions

- Lab - Qwest Diagnostic Laboratory facilities.
- Negative - Test results of screens that do not prove the presence of drugs, alcohol, and/or controlled substances.
- Negative-Dilute - Test results of screens where the test sample is outside the “normal” range.
- Positive - Test results of screens that prove the presence of drugs, alcohol, and/or controlled substances.
- Medical Review Officer (MRO) - The MRO reviews and confirms all negative and positive test results.

- Substance abuse - The misuse or unlawful use of drugs (prescribed or otherwise, alcohol, and/or controlled substances).

X. Smoke-/Tobacco-free Workplace

VSP Vision ("VSP") is committed to providing a safe and healthy workplace and to promoting the health and well-being of our Contingent Workers or Service Providers. The following Smoke-/Tobacco-Free Workplace Policy ("Policy") applies to all Contingent Workers or Service Providers, contingent workers, student interns, and visitors to VSP facilities. VSP prohibits smoking and other tobacco related use at all facilities within the United States during work and/or work hours. The Policy includes, but is not limited to:

- Lighting, smoking or carrying a lighted or smoldering cigarette, cigar, or pipe of any kind
- e-Cigarettes
- Vaping
- Chewing tobacco and tobacco-free products
- All personal vehicles while parked on company-owned property, parking lots, walkways and common areas
- All vehicles owned or leased by the company – i.e. cars, trucks, vans, mobile coaches
- VSP Leased Properties

Unless specified within the leasing contract, VSP cannot mandate a smoke-/tobacco-free worksite. However, Company policy requires Contingent Workers or Service Providers, contingent workers, student interns, and visitors who choose to smoke, use e-cigarettes, vape, and/or partake of tobacco products to do so a minimum of fifty (50) yards from any building entrance/exit.

Mobile Response Events

This Policy extends to remote work environments established as a result of the Company's mobile response efforts. Contingent Workers or Service Providers participating in these efforts who choose to smoke, use e-cigarettes, vape, and/or partake of tobacco products are required to adhere to the aforementioned fifty (50) yard minimum distance away from the event activities.

Breaks

Regularly scheduled breaks cannot be extended to allow Contingent Workers or Service Providers to leave the facility to smoke and/or use e-cigarettes, vape, and/or partake of tobacco products during working hours. No additional time from work shall be authorized for such activity.

Smoking Cessation Resources

VSP sponsors a comprehensive smoking cessation program that includes onsite smoking cessation classes offered at no cost to Contingent Workers or Service Providers and their dependents. There are also online and telephonic options, as well as a reimbursement program for alternative cessation methods. For details, see Smoking Cessation Program Resources on Globalview.

Responsible Corporate Citizens

If you choose to smoke during your breaks, please do so in/on public domain areas only. As a VSP Vision Contingent Workers or Service Providers, you are responsible for ensuring those areas remain clean and free of cigarette butts and/or other debris.

Compliance

Management staff will be responsible for ongoing compliance with the Policy. They are expected to adhere to standard practices in resolving issues of conformance and maintaining expected levels of work productivity. Violation of this Policy may result in disciplinary action, up and including termination.

XI. Gender Identity & Expression Policy

VSP complies with Title VII of the Civil Rights Act of 1964, and all applicable state and local fair employment practices laws and is committed to providing equal employment opportunities to all individuals, regardless of their sex [sexual orientation, gender identity or gender expression]. Consistent with this commitment, VSP strives to create a safe and productive workplace environment for all Contingent Workers or Service Providers. This Policy sets forth guidelines to address the needs of transgender and gender conforming Contingent Workers or Service Providers, and supports VSP's Equal Opportunity, Anti-Harassment and Anti-Discrimination policies (which include gender identity and gender expression).

Names and Pronouns

A Contingent Workers or Service Providers has the right to be addressed by the name and pronoun that correspond to the Contingent Workers or Service Provider’s gender identity, upon request. Managers, supervisors, and coworkers should take care to use the correct name and pronouns in communications with the Contingent Workers or Service Providers, as well as when addressing others regarding the Contingent Workers or Service Providers. Continued intentional misuse of a Contingent Workers or Service Provider’s new name and pronouns, and reference to the Contingent Workers or Service Provider’s former gender by managers, supervisors, or coworkers is contrary to the goal of treating Contingent Workers or Service Providers with dignity and respect, and creates an unwelcoming work environment.

Contingent Workers or Service Providers Records

VSP will change a Contingent Workers or Service Provider’s official record to reflect a change in name or gender upon request from the Contingent Workers or Service Providers. Certain types of records, like those relating to payroll and retirement accounts, may require a legal name change before the person's name can be changed. Some records, however, can be changed to reflect a person's preferred name without proof of a legal name change.

If a new or transitioning Contingent Workers or Service Providers has questions about company records or ID documents, the Contingent Workers or Service Providers should contact Human Resources.

Restroom and Locker Room Accessibility

All VSP Contingent Workers or Service Providers have a right to safe and appropriate restroom facilities, including the right to use a restroom that corresponds to the Contingent Workers or Service Provider’s gender identity or gender expression, regardless of the Contingent Workers or Service Provider’s sex assigned at birth. The decision of which facility to use will be left to the Contingent Workers or Service Providers to determine the most appropriate and safest option for them.
Furthermore, no Contingent Workers or Service Providers will be required to undergo, or provide proof of, any medical treatment or procedure, or provide any identity document, to use facilities designated for use by a particular gender.

Dress Codes

Our company does not have dress codes that restrict Contingent Workers or Service Providers' clothing or appearance on the basis of gender. Contingent Workers or Service Providers have the right to comply with company dress codes in a manner consistent with their gender identity or gender expression.

Discrimination / Harassment

It is unlawful and violates company policy to discriminate in anyway (including, but not limited to, failure to hire, failure to promote, or unlawful termination) against a Contingent Workers or Service Providers because of the Contingent Workers or Service Provider's actual or perceived gender identity. Additionally, it also is unlawful and contrary to this policy to retaliate against any person objecting to, or supporting enforcement of legal protections against, gender identity discrimination in employment.

VSP is committed to creating a safe work environment for transgender and gender conforming Contingent Workers or Service Providers. Any incident of discrimination, harassment, or violence based on gender identity or expression will be given immediate and effective attention, including, but not limited to, investigating the incident, taking suitable corrective action, and providing Contingent Workers or Service Providers with approprite resources.

XII. Prohibited Behavior

The following conduct is prohibited while on assignment for VSP, while on company property, or while in a company facility or vehicle:

- Unauthorized use, possession, or concealment of alcohol
  - Being under the influence of alcohol or drugs to the degree that it impairs judgment, performance, or conduct, including being convicted of operating a motor vehicle while under the influence of alcohol or drugs.
  - Unlawful use, possession, concealment, manufacture, sale, solicitation, purchase, dispensation or distribution of drugs or controlled substances.

- Service Provider responsibility
  - Contingent Workers or Service Provider must notify their onsite supervisor and employer of any drug-related convictions and/or any convictions for operating a company vehicle while under the influence of alcohol or drugs or while on assignment for VSP.

- Reasonable Suspicion
  - If a Contingent Workers or Service Provider is behaving in an impaired or unsafe manner, or there is other reasonable cause to believe he/she has engaged in the misuse or illicit use of alcohol, drugs or controlled substances, the Contingent Worker or Service Provider will be referred to the appropriate lab for screening.

- Post-Accident
  - A post-accident test for alcohol and/or drugs will be required for any assignment-related accident, assignment-related incident involving an injury to the Contingent Worker or Service Provider or a third party or property; involving operation of machinery (e.g. forklift, WAVE, company-owned motor-vehicle) causing significant property damage or injury or if there is "reasonable suspicion" or the apparent violation of a safety rule or standard. The Contingent Worker or Service Provider will be referred to the appropriate lab for screening.

Disciplinary Action for Violations

Violation	Consequence
Unauthorized use, possession or concealment of alcohol on company time or property	Disciplinary action up to and including termination of service
Impairment of judgment, performance, or conduct due to the influence of alcohol and/or drugs on company time or property	Disciplinary action up to and including termination of service
Unlawful use, possession, concealment, manufacture, sale, solicitation, purchase, dispensation or distribution of drugs or controlled substances on company time or property	Termination of service
Failure to report prohibited convictions	Termination of service
Refusal to consent to drug testing and referral for reasonable suspicion	Termination of service

XIII. Access to Computing Resources

Contingent Workers or Service Providers and contingent workers at a VSP location or remotely must follow computing resources access rules and privileges.

Training on security awareness, privacy and teleworker responsibilities will be required prior to teleworking authorization.

Contingent Workers or Service Providers will be required to acknowledge they have received training and are aware of their responsibilities through sign-off.

VSP's Contingent Workers or Service Providers are provided with the organization's data privacy and security policy prior to accessing system resources and data.

VSP will establish policies and/or standards so that usage is explicitly authorized and acceptable usage defined, including (i) explicit management approval (authorization) to use the technology; (ii) authentication for the use of the technology; (iii) acceptable uses of the technologies, with special emphasis on the inappropriate access by workers to personal information of neighbors, colleagues and relatives; (iv) acceptable network locations for the technologies; (v) list of VSP-approved products, including cloud-based services for usage and the storage of VSP data; (vi) activation of modems for vendors only when needed by vendors, with immediate deactivation after use; and, (vii) prohibition of storage of covered data onto local hard drives, floppy disks, or other external media.

Network Access

VSP maintains network security by controlling who does and does not have access to our network. All access must be requested and approved by your manager. Only company- managed Workplace Devices, as described in the Acceptable Use section, are permitted to access the corporate network.

Guest Access

Personal devices belonging to VSP Contingent Workers or Service Providers, contractors or third parties may be granted access to a Guest network based on business needs.

Remote Access

VSP will evaluate the physical security of the teleworking site (e.g., the building and local environment) and address threats/issues prior to authorization (e.g., unauthorized access to information or resources from other persons using the accommodation, such as family and friends).

VSP will address the following matters prior to authorizing teleworking: (i) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access; (ii) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of VSP is not allowed; (iii) the provision of suitable communication equipment, including methods for securing remote access; (iv) rules and guidance on family and visitor access to equipment and information; (v) the provision of hardware and software support and maintenance; (vi) the procedures for back-up and business continuity; (vii) the provision of a means for teleworkers to communicate with information security personnel in case of security incidents or problems; (viii) audit and security monitoring; and, (ix) any organization-owned equipment is used only for business purposes by authorized Contingent Workers or Service Providers.

Everyone authorized to access the network remotely must do so in approved ways. Access must be requested through Service Central and approved by your manager. Acceptable ways to access our network remotely include:

- Virtual Private Network (VPN) when connecting from a Workplace Device.
- Virtual Desktop Infrastructure (VDI) if connecting from a personal device.

Follow your Internet Service Provider or manufacturer's recommendations to enable encryption on your personal wireless router and set a strong password. Connect to the VPN at least once per week to receive software and security updates. For added security, the VPN is configured to disconnect automatically after a pre-determined time and requires you to reauthenticate by entering your user credentials.

VSP instructs all personnel working from home to implement fundamental security controls and practices, including, but not limited to, passwords, virus protection, personal firewalls, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate worksites.

Account Privileges

Your manager will assign a user profile with appropriate access to programs and information. Some work duties may require the assignment of a separate Administrator account with elevated privileges to effect change to a system.

Contractors will be provided with the minimal system and physical access and will agree to and support the organization's security requirements. The contractor selection process will assess the contractor's ability to adhere to and support the organization's security policy and procedures.

Having more privileges than necessary or using a separate Administrator account inappropriately can expose you and the company to unnecessary risk. Accounts with administrator privileges must not be used for routine work tasks, like accessing email.

At regular intervals, your manager will review and approve your access rights. If your duties have changed, you may have access removed or added. If you know you have access you no longer require, you should notify your manager.

Users will sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group.

Users will be given a written statement of their access rights, which they are required to sign stating they understand the conditions of access. Guest/anonymous, shared/group, emergency and temporary accounts are specifically authorized and use monitored.

Multi-factor Authentication

VSP requires multi-factor authentication (MFA) when accessing your Office 365 account. Additionally, multi-factor authentication may be required for accessing certain information systems. VSP implements multi-factor authentication using "something you know" and "something you have":

- The "something you know" is your unique username and strong password/passphrase.
- The "something you have" is a one-time passcode or voice call to your mobile phone or a special hardware security device issued to you.

To set up multi-factor authentication on your Workplace Device and mobile phone, follow the step-by-step instructions in this Knowledge Base Article: Set Up Multi-Factor Authentication (MFA) to receive verification phone call using computer (Quick Guide).

Password Security

You can help defend the VSP network and protect our information by setting strong passwords or using a passphrase. VSP automatically enforces password rules to defend against password guessing and brute-force attacks.

Remember these guidelines to create an effective password that meets VSP security requirements:

- Use a passphrase with at least 14 characters; longer passphrases are far more difficult to crack.
- Make it unique and memorable to you; avoid using personal information like your birthdate or middle name.
- Don't use the same password for personal and business account logins; if your password is compromised, it could mean your other accounts are exposed as well.
- Make it complex; use at least 3 elements - UPPER case, lower case, number, and special characters and spaces count too. Here is an example of a good passphrase: (but please don't use it): I H3lp People $ee!

Additional protections for your passwords include:

- Preventing reuse of previous 12 passwords.
- Resetting passwords every 120 days to prevent a determined attacker from guessing a password before it expires.
- Locking accounts after 8 consecutive failed attempts.
- Keeping accounts locked for 10 minutes unless unlocked by an administrator.
- Locking your Workplace Device after 15 minutes of inactivity requiring you to enter your password to unlock it.

VSP does not permit the use of shared or "group use" accounts and passwords to access systems and information.

No one should ever ask you for your password, including help-desk and technical support personnel. Never share your password or allow someone else to use your account. Never write down your password or keep it in a place where it would be easily observed.

Resetting a Password

Everyone must register with Self-Service Password Reset Tool to manage lockouts and password resets. The Self-Service Password Reset Tool applies to VSP Contingent Workers or Service Providers only. Marchon Contingent Workers or Service Providers, please contact the Service Desk for all password reset incidents. On the VSP Network? You can continue to change your password on your computer log-in screen.
To get started, go to: https://myaccount.microsoft.com, or the password reset link on insidevsp.com, and follow

the steps below:

- Select *"Change Password."*
- Follow the verification steps to reset your password.
- Need help? Follow the step-by-step instructions in this Password Reset Knowledge Base Article. After you've successfully updated your password, you can reset it from anywhere by visiting insidevsp.com and choosing the **"Microsoft Azure Password Reset"** link.

XIV. Acceptable Use of Workplace Devices

This section outlines what you can and can't do when using VSP's Workplace Devices and accessing our information assets. It describes the safe and responsible computing behavior we expect and monitors while working at VSP, whether onsite or remotely. All Contingent Workers or Service Providers and contingent workers using our Workplace Devices must follow this standard.

VSP will develop, disseminate, and annually review/update a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements for its human resources security protection program (e.g., through policy, standards, guidelines, and procedures). Further, VSP will document procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Contingent Workers or Service Providers, contractors, and third-party users using or having access to the organization's assets will be aware of the limits existing for their use of the organization's information and assets associated with information processing facilities and resources. Users will be responsible for their use of any information processing resources and for any such use carried out under their responsibility.

VSP will establish policies and/or standards so that usage is explicitly authorized and acceptable usage defined, including (i) explicit management approval (authorization) to use the technology; (ii) authentication for the use of the technology; (iii) acceptable uses of the technologies, with special emphasis on the inappropriate access by workers to personal information of neighbors, colleagues and relatives; (iv) acceptable network locations for the technologies; (v) list of VSP-approved products, including cloud-based services for usage and the storage of VSP data; (vi) activation of modems for vendors only when needed by vendors, with immediate deactivation after use; and, (vii) prohibition of storage of covered data onto local hard drives, floppy disks, or other external media.

Management responsibilities will ensure that Contingent Workers or Service Providers, contractors and third-party users: (i) are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems; (ii) are provided with guidelines to state security expectations of their role within VSP; (iii) are motivated and comply with the security policies of the organization; (iv) achieve a level of awareness on security relevant to their roles and responsibilities within the organization; (v) conform to the terms and conditions of employment, which includes VSP information security policy and appropriate methods of working; and, (vi) continue to have the appropriate skills and qualifications.

Communication to all Contingent Workers or Service Providers will notify them that their actions may be monitored and that, through signing an acceptable use agreement, they have consented to such monitoring (Note: the legality of such monitoring will be verified in each legal jurisdiction).

VSP will provide notice that the Contingent Workers or Service Provider's actions may be monitored and that the Contingent Workers or Service Providers consents to such monitoring.

VSP will establish and make readily available to all information system users a set of rules that describe their responsibilities and expected behavior regarding information and information system usage. Further, acceptable use will address rules for electronic mail and Internet usage; and guidelines for the use of mobile devices, especially for use outside the premises of VSP. VSP will include in the rules of behavior explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.

All Contingent Workers or Service Providers and contractors will be informed in writing (e.g., when they sign rules of behavior or an acceptable use agreement) that violations of security policies may result in sanctions or disciplinary action.

VSP includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action. VSP employs a formal sanctions process for personnel failing to comply with established information security policies and procedures and notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction.

VSP-Provided Workplace Devices

To perform your work, we may entrust you with:

- A computer such as a desktop, laptop, or tablet to access our network or the Internet.
- A desk phone to make and receive calls.
- A mobile phone to access your calendar, email, and other tools, depending on your role.
- Other devices such as a USB drive, Webcam, WiFi hotspot, or printer.
- Access to software, like softphones, servers, or other information assets on our network.

Users of mobile computing devices in public places will take care to avoid the risk of overlooking by unauthorized persons. Training will be arranged for personnel using mobile computing to raise their awareness of the additional risks resulting from this way of working and the controls that are implemented.

Together, these computers, phones, devices, networks, and software are called “Workplace Devices.” Whether you work at a VSP location or from your home office, you’re responsible for using Workplace Devices for work-related activity and for limited, reasonable, and essential personal use. We’ll define acceptable personal use later in this standard.

At the end of your assignment or employment with VSP, you must return all Workplace Devices to us. Your manager will collect these or arrange for pickup at your home if needed.
VSP will implement the following teleworking arrangements: (i) teleworking activities are formally managed/controlled and only authorized if suitable security arrangements and security controls that comply with relevant security policies and VSP requirements are in place; (ii) the communications security requirements are addressed and take into account the need for remote access to VSP internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system.; (iii) the use of home networks and requirements/restrictions on the configuration of wireless network services including encryption (AES WPA2 at a minimum) are addressed; (iv) antivirus protection, operating system and application patching, and firewall requirements consistent with corporate policy are addressed; (v) revocation of authority and access rights and the return of equipment when the teleworking activities are terminated are addressed; (vi) verifiable unique IDs are required for all teleworkers accessing VSP’s network via a remote connection; (vii) the connection between VSP and the teleworker’s location is secured via an encrypted channel; and, (viii) VSP maintains ownership over the assets used by the teleworker in order to achieve the requirements of this control.

Personal Use

We expect everyone to use Workplace Devices honestly and for work-related purposes. Personal use must not affect VSP business, impact your productivity, or jeopardize the security of Workplace Devices. Any personal use must be:

- **Limited** — meaning your use is *temporary* and *specific* to an important task;
- **Reasonable** — meaning your use is *sensible* and *not excessive* given the circumstances; and
- **Essential** — meaning your use is *required* to do an important task.

Here are examples of limited, reasonable, and essential personal use:

- Checking the hours of a pharmacy before picking up a prescription.
- Calling a family member to let them know you're running late.
- Looking up flight status of arrival for a friend or family member.

If you're not sure if a specific activity is acceptable, use these questions to guide you. *Am I following company policy? Can I defend my actions to my manager? Am I protecting the information of our doctors, members, clients and Contingent Workers or Service Providers? Am I protecting the information of VSP?*

VSP will formally document policies and/or standards related to BYOD usage to meet the following requirements, as applicable to the organization: (i) clearly identifies applications, application stores and application extensions and plugins approved for bring your own device (BYOD) usage; (ii) defines the device and eligibility requirements to allow for BYOD usage; (iii) clarifies its expectations of privacy and its requirements for litigation, e-discovery, and legal holds with respect to mobile devices; (iv) clearly states expectations regarding the loss of VSP data in case a wipe of a mobile device is required; and, (v) clarifies the systems and servers allowed for use or access on a BYOD-enabled device.

Using the Internet. The Internet is an inherently dangerous place and an easy way for attackers to load malicious software that can harm VSP computing resources. While we have reasonable safeguards to protect you while on the VSP network, no security system is perfect. We can't guarantee security while connected to the Internet. That's why it's important for each of us to protect what we've been entrusted with. This includes limiting your use of the Internet. You must not use Workplace Devices as a personal device or to:

- Check your personal email.
- Register and manage personal accounts (utilities, entertainment, bank accounts)
- Shop online for personal items.
- Stream movies or music for entertainment.

VSP will establish policies and/or standards so that usage is explicitly authorized and acceptable usage defined, including (i) explicit management approval (authorization) to use the technology; (ii) authentication for the use of the technology; (iii) acceptable uses of the technologies, with special emphasis on the inappropriate access by workers to personal information of neighbors, colleagues and relatives; (iv) acceptable network locations for the technologies; (v) list of VSP-approved products, including cloud-based services for usage and the storage of VSP data; (vi) activation of modems for vendors only when needed by vendors, with immediate deactivation after use; and, (vii) prohibition of storage of covered data onto local hard drives, floppy disks, or other external media.

Storage of Personal Files. You must not download or store personal files on Workplace Devices, including photos, documents, and music. If you do, don't assume they're private. We may remove them at any time without notice and won't recover them once removed.

Expectation of Privacy. Everyone using or accessing VSP information assets must follow the organization's security rules to guard against accidental or intentional abuse within our organization. You have no right to privacy in your use of Workplace Devices, whether you are working at VSP, at home, or when traveling. We reserve the right to review all activity on Workplace Devices. VSP actively monitors Internet usage, policy compliance, and job performance statistics. If activity on your device is deemed to be excessive, negligent or malicious, disciplinary action may be taken.

Unacceptable Uses

This list of unacceptable behavior is not intended to be exhaustive. If you're not sure if something is unacceptable, or if you see someone else using Workplace Devices in these ways, talk to your manager or contact Human Resources.

Management will approve the use of information assets. If any unauthorized activity is identified by monitoring or other means, this activity will be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Illegal, Offensive, and Fraudulent Activity. You must not use Workplace Devices in any way that is unlawful, offensive, fraudulent, or infringes the rights of others. Examples include:

- An illegal activity like child pornography, gambling, piracy, or violating intellectual property laws.
- Offensive activity involving defamatory, obscene, abusive, or otherwise objectionable content.
- Fraudulent activity includes offering fraudulent goods or services, schemes, or phishing.

Bypassing Security. We secure Workplace Devices to protect members, customers, you and VSP. Bypassing security can put us all at risk. You must not violate Workplace Devices by trying to bypass security measures. Examples include:

- Using Workplace Devices without permission or in an unacceptable way.
- Using Workplace Devices in a way that could disable, overburden, damage, or impair it.
- Intentionally uploading, downloading, transmitting, storing, reproducing, or distributing a computer virus, worm, or any other malicious computer code.

Abusing Our Network. Our network runs our business. Without it, we can't achieve our mission to help people see. You must not violate the security, integrity, or availability of our network.

Examples include:

- Monitoring or intercepting network traffic without permission.
- Intentionally interfering with our network or its performance.
- Hacking our network to gain unauthorized access to information assets, data or other Workplace Devices.

VSP will identify a point of contact from HR to handle any incidents relating to Contingent Workers or Service Providers. VSP will also notify the CISO or a designated representative of the application of a formal Contingent Workers or Service Providers sanctions process, identifying the individual and the reason for the sanction.

Abusing Email. Emails are company records and our email addresses are VSP property. Our email system is only meant for business communications. You must not use your company- issued email address to:

- Send spam or send unsolicited advertising or promotional messages.
- Send chain mail.
- Register a personal online account for goods or services not required for business purposes
- Forward restricted or confidential business emails to a personal account. For more about information types, see the Information Classification and Handling Standard.

Protecting Workplace Devices

We've configured Workplace Devices to secure them and help you perform your work. Protections range from restricting privileged access to encryption and firewalls. We also install updates regularly to ensure devices are protected from the latest threats. You must not remove, alter, or disable any security software or prevent security updates from being installed.

Approved Software. The software can be dangerous. It can have backdoors or other flaws that expose VSP to hackers. That's why it's important you only use approved, supported software to do your job. We maintain an approved list of software to ensure compliance with licensing agreements and security concerns. If you require additional software, plugins, cloud- based applications, or utilities, you must submit a request through Service Central.

You must not install software without first getting approval. Any unauthorized software detected on Workplace Devices may be subject to removal.

VSP will prohibit users from installing unauthorized software, including data and software from external networks, and will ensure users are made aware and trained on these requirements.

Clear Desk, Clear Screen. Whether you work at a VSP facility or remotely, you're responsible for protecting VSP information by keeping your workspace clear of plainly seen confidential information. This includes locking your screen when you walk away from your desk and making sure paper copies of confidential information are locked in your desk or a cabinet. Shut down and secure your Workplace Device when storing it overnight. Paper documents that are no longer required must be shredded by depositing them in a shred bin or using a cross-cut shredder. Never put confidential information in a recycle or trash bin.

Hold meetings and phone conversations of a sensitive or confidential nature in a private

space. When you are working away from the office, be aware who can see your monitor when in public places or open workspaces. Use a privacy screen to protect against shoulder surfing.

When transporting your Workplace Device, keep it in the trunk of your vehicle. Never store it where it can be seen through a window.

VSP will ensure covered or critical information is protected when using internal or external (e.g., USPS) mail services, including if information will not be visible through envelope windows, and envelopes will be marked according to their classification level (e.g., confidential). Additionally, incoming and outgoing mail points and unattended facsimile machines are protect

Covered critical business information (e.g., on paper or on electronic storage media) will be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Additionally, computers and terminals will be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism that conceals information previously visible on the display when unattended and will be protected by key locks, passwords or other controls when not in use. Documents containing covered or classified information will be removed from printers, copiers, and facsimile machines immediately, and when transporting documents with covered information within facilities and through inter-off.

XV. Electronic Equipment Policy

VSP Global® (VSP) may furnish Contingent Worker or Service Provider with electronic and communication equipment/systems and software for the use and benefit of VSP and it's business partners. Every user is responsible to use the equipment/systems in a productive, ethical, and lawful manner. This policy pertains to all computers, virtual communication tools, software, telephones (desktop and cellular), wearable technology, FAX machines, printers, copiers, pagers, audio/visual equipment, or any other electronic equipment or device (collectively "Electronic Equipment") issued by the Company. Minimal use of VSP's Electronic Equipment for informal/personal purposes or outside regular assignment hours is permissible only with on-site supervisor and VSP management approval and within reasonable time limits.

Business Etiquette

All forms of communications must be courteous, professional, business-like, and must represent VSP appropriately. Use of VSP's Electronic Equipment to transmit or receive chain letters and defamatory, obscene, discriminatory, illegal, offensive, threatening, intimidating or harassing material or messages is strictly prohibited.

Telephone

- You are the voice of the VSP and should treat everyone with the respect he or she deserves.
- Greet your caller in a friendly and professional manner including your name and the name of the company.
- For extended absences, away from your desk, create an out-of-office reply that includes your status, when the recipient can expect your return, and accurate instructions for an alternative contact.
- Make personal calls at lunch or during break times whenever possible.

Company-supplied equipment

Contingent Worker or Service Provider in certain job assignment may be issued a smart phone, laptop, data card, and/or tablet device ("Device"). The following applies to all Devices:

- Device must be passcode protected and the user must notify the Technical Assistance Center (TAC) at 916.851.4500 in the event the Device is lost or stolen. The Device will be remotely "wiped" of all information and applications when it is reported missing.
- Contingent Worker or Service Provider in possession of a Device are expected to protect the Device from loss, damage, misuse, loading of unauthorized software, or theft.
- Upon termination of service or any time upon request, the Contingent Worker or Service Provider must return the

  Device for return or inspection.
- Contingent Worker or Service Provider are expected to adhere to applicable laws regarding use of cell phones while driving.

Company-supplied Laptops

- Laptops will be provided to Contingent Worker or Service Provider who have an appropriate business need.

Privacy—Electronic Communications

- Contingent Workers or Service Providers have no right of privacy in communications performed on company-owned equipment or systems. All electronic communications and systems may be reviewed by authorized personnel. Periodic monitoring of Internet usage is conducted. If it is determined to be excessive and not for legitimate business reasons, the Service Provider's assignment will be terminated.

Remote User Security

- Contingent Worker or Service Provider assigned to VSP may require remote access to VSP networks. You will be notified whether your assignment requires remote access.
- It is the responsibility of the remote access user to ensure that his/her remote access connection is treated in a responsible and secure manner and used only for VSP-related business activities. Remote access of VSP's network for recreational use by the Contingent Worker or Service Provider or Contingent Worker or Service Provider at the remote access site is strictly prohibited.

Software and File Storage - Copyrights/Licensing/Usage

The use of the Internet to download applications is prohibited. If a Contingent Worker or Service Provider must download an application, the Contingent Worker or Service Provider must obtain prior written approval from Global Technology Services (GTS). Unauthorized copying of any software is a violation of U.S. copyright law and may constitute a crime punishable by a fine of up to $250,000 and imprisonment for up to five years.

VSP purchases licenses for all software used by the Company. Under no circumstances should (1) company software be installed on any computer without verification that a license has been purchased for that application, or (2) software be installed on company equipment without written authorization from GTS management. For the security and protection of VSP systems and to ensure licensure compliance, GTS will conduct all software downloading.

Contingent Workers or Service Providers may store personal files on the local "C" drive (not in the My Documents folder). Contingent Workers or Service Providers must create a personal folder on the ROOT of the "C" drive. Be aware that folders on the ''C" drive are not backed up on company servers and data cannot be recovered if lost. Also, do not assume that these files are private. Storage of personal files, including photos, movies, and music files on any other drive is prohibited. The company may remove personal files from all networked storage devices without notice at any time.

VSPOne Personal Electronic Device Policy (except VSPOne Sacramento)

Personal electronic devices are a distraction in the workplace and may create a safety hazard and interfere with productivity. For purposes of this policy, “personal electronic devices” are defined as any device that makes or receives phone calls, leaves messages, sends text messages, surfs the Internet, downloads and allows for the reading of and responding to email, or creates or plays pictures, video, or sound recordings.

Contingent Workers or Service Providers are not permitted to use personal electronic devices, including “listening only” devices while operating any company equipment or in any production area of the facility. Production areas are defined as all equipment areas, pre-production, customer service, maintenance, admin and support workstations. Personal electronic devices should not be visible at work stations.

Personal electronic devices may be used during regular breaks and lunch periods in designated production areas such as the break room or outside the building. Each VSPOne location will provide a method for contact of the Contingent Workers or Service Providers in case of emergency. Exceptions may be made on a case-by-case basis by the Contingent Workers’ or Service Providers’ on-site supervisor.

Personal electronic devices should never be connected to company computers or other company equipment. Personal electronic devices should be charged at designated charging locations only.

Company policy and privacy regulations require that confidential and proprietary information be protected. For this reason, Contingent Workers or Service Providers shall not use any device to record sound, pictures, or video in any area of the facility.

The Company will not be liable for the loss of personal electronic devices brought into the workplace.

Certain Contingent Workers or Service Providers, such as supervisors, leads, and maintenance personnel routinely use personal electronic devices to conduct business. Nothing in this policy is intended to restrict such business use.

XVI. Fraternization Policy

VSP Global® (VSP) strongly discourages fraternization by management with Contingent Workers or Service Providers who are assigned directly or indirectly to their team. While it is impossible to specify all situations which may give rise to fraternization problems, some common examples of inappropriate fraternization between management and Contingent Workers or Service Providers include, but are not limited to: dating, cohabitation, excessive social activities (excluding business gatherings or meetings), or interactions on social media.

Personal relationships between a member of management and a Contingent Workers or Service Providers may give rise to perceptions of favoritism, could lead to claims of conflict of interest, sexual harassment, or discrimination, and lowers morale. It is the responsibility of management to avoid fraternization and to use discretion and good judgment relating to activities and interactions with Contingent Workers or Service Providers outside of the workplace.

Any Contingent Workers or Service Providers who becomes aware of a potential violation of this policy must bring it to the attention of their on-site supervisor, employer or Human Resources (HR) immediately. All information will be kept confidential on a need-to-know basis. HR will work with on-site supervisor and/or employer to facilitate a resolution of the situation, which may involve a transfer, demotion, or disciplinary action up to and including termination of service for both parties.

XVII. Fraud, Waste and Abuse Policy

VSP Global® (VSP) prides itself on the integrity of the organization, its Contingent Workers or Service Providers, and its health care providers. Thus, it is the policy of VSP to detect and report any and all types of fraudulent or abusive activity, including insurance fraud and criminal conduct in all forms practiced by health care providers, contract laboratories, VSP Contingent Workers or Service Providers, Contingent Workers, Service Providers, clients, agents and patients. It is further the policy of VSP to consistently and fully comply with all laws and regulations pertaining to the delivery of and billing for services which apply to VSP on account of its participation in Medicare, Medicaid and other government programs, and to fully cooperate with law enforcement and regulatory bodies

Introduction

VSP has developed a Fraud, Waste and Abuse Program to be a comprehensive statement of the responsibilities and obligations of all Contingent Workers or Service Providers regarding all types of insurance fraud, criminal or unethical activity, and submissions for reimbursement to Medicare, Medicaid, and other government payers for services rendered by VSP and any of its subsidiaries, divisions, health care providers, contract laboratories and agents.

Contingent Workers or Service Providers Participation and Reporting

It is the responsibility of every Contingent Workers or Service Providers to abide by applicable laws and regulations and support VSP's compliance efforts. VSP has prepared an Anti-Fraud, Waste and Abuse Policy C-0004 which outlines the procedures under which the Anti-Fraud, Waste and Abuse Program will operate. It is the responsibility of every Contingent Workers or Service Providers to review the policy and participate in the program.

All Contingent Workers or Service Providers are required to report their good faith belief of any violation of the Anti-Fraud, Waste and Abuse Program or applicable law. If the Contingent Workers or Service Providers requests, VSP will provide such anonymity to the Contingent Worker(s) or Service Provider (s) who report as is possible under the circumstances, consistent with its obligations to investigate Contingent Workers or Service Providers concerns and take necessary corrective action. There shall be no retaliation for making a report.

Contingent Workers or Service Providers may report violations of the compliance program or applicable laws either (i) orally or in writing to their manager; (ii) by calling the Special Investigative Unit at (916) 851-6500 or the VSP Chief Compliance Officer at (916) 858-5446; (iii) by mailing their written concern to VSP Special Investigative Unit, Mail Stop 913, 3333 Quality Drive, Rancho Cordova, CA 95670; or (iv) by calling the VSP Anti-Fraud, Waste and Abuse hotline at (800) 877-7236.

Responsible Officer

VSP has designated Dan Schauer, Global Corporate Finance and Risk Officer, as the Chief Compliance Officer. The Chief Compliance Officer is the individual within VSP responsible for the overall implementation and operation

of the VSP Anti-Fraud, Waste and Abuse Program. The Chief Compliance Officer shall report in writing annually to the Audit Committee of the Board of Directors on the status of the VSP Anti-Fraud, Waste and Abuse Program.

XVIII. Regulatory Compliance & Regulators

VSP Global® (VSP) provides varied healthcare services in many states. Generally, these services are subject to federal and state laws and regulations and may require the Company to comply with certain obligations such as: certificates of need, licenses, permits, accreditation, access to treatment, consent to treatment, medical record-keeping, access to medical records and confidentiality, members' rights, VSP doctor privileges, corporate practice of medicine restrictions, and Medicare and Medicaid regulations. VSP is subject to numerous other laws and regulations in addition to the above.

VSP complies with all applicable laws and regulations and its Regulatory Compliance department monitors, assesses, and addresses compliance issues. All Contingent Workers or Service Providers must strive to comply with all laws and regulations pertaining to their job responsibilities and should immediately report any violations or suspected violations to your on-site supervisor, employer management, the Office of the General Counsel, the Corporate Ethics and Compliance Officer, the Regulatory Compliance department at RegulatoryManagement@vsp.com, or you may also contact the confidential toll-free Ethics Reporting Hotline, at 1-877-349-7494.

VSP will be forthright, open, and honest in dealing with any governmental inquiries. Requests for information will be answered with complete, factual, and accurate information. We will cooperate with and be courteous to all government auditors, investigators and inspectors and provide them with the information to which they are entitled during an inquiry.

During a government inquiry, you must never conceal, destroy, or alter any documents, lie, or make misleading statements. You should not attempt to cause another Contingent Workers or Service Providers to fail to provide accurate information or obstruct, mislead, or delay the communication of information or records relating to any inquiry.

The scope of matters related to regulation and licensing are significant and broader than the scope of this Code of Conduct. If you are contacted by a regulatory and/or licensing body and have questions, please call the Office of the General Counsel at (916) 852-7600 for assistance.

XIX. Ownership of Inventions and Work Product Policy

As a VSP Global®Contingent Workers or Service Providers, you may be called on from time to time to participate in developing or inventing new products or procedures for the Company. Any work product or invention created by you as a Contingent Workers or Service Providers within this relationship is the property of VSP; this includes, but is not limited to, inventions, patents, any copyrightable works, computer programs or applications, or business procedures, processes, operations, or programs, and related materials.

XX. Workplace Searches Policy

In keeping with the spirit and intent of VSP Global®'s (VSP) goal to safeguard the property of our Contingent Workers or Service Providers, Contingent Workers or Service Providers, customers, and company, VSP reserves the right to inquire about and/or inspect any boxes, packages, and backpacks that are in the possession of Service Providers, contractors, vendors, and guests as they enter or leave our premises.

In conjunction with implementing this policy, VSP has posted notices of said policy in conspicuous places throughout our facilities.

When removing VSP property from the premises (excluding company-assigned items, such as cell phones, laptops, etc.), Contingent Workers or Service Providers are reminded that they must obtain and complete a Property Pass. The pass must be signed by their onsite supervisor or department manager authorizing the removal of company property.

Contingent Workers or Service Providers and contractors who refuse to cooperate in an inspection, or are in possession of stolen property, will be subject to disciplinary action up to and including termination of service. Vendors and guests

entering the premises who refuse to cooperate in an inspection conducted pursuant to this policy will not be permitted to enter the premises.

XXI. Workplace Violence Policy

Purpose

VSP Global®(VSP) is committed to providing a safe work environment for all Contingent Workers or Service Providers. Threats or acts of violence will not be tolerated and are grounds for immediate dismissal. All Contingent Workers or Service Providers must promptly report to on-site supervisor, employer, and/or VSP management any situations involving actual or potential violence.

Service Provider's Responsibility

Strictly adhere to VSP's workplace violence policy as outlined above. If there is potential for imminent violence (such as visible weapons or explosives), and your onsite supervisor or other management personnel are not immediately available, call 9-911 for local law enforcement, followed by VSP Global® corporate security at 916.858.7345. Security is staffed 24/7.

At a minimum, be prepared to provide the following information:

- Names of perpetrator involved in the hostile incident
- Nature of the incident
- Number of victims
- Condition of the victims (i.e., whether their injuries appear to be life threatening)
- Presence of any hazards at the scene (i.e. weapons, explosives, chemicals, etc.)
- Names of all witnesses to the incident

Refrain from making any statement to internal and external personnel and news media regarding the incident. All inquiries or comments should be referred to an authorized company spokesperson.

Additionally Referenced

XXII. Corporate Ethics and Compliance Program

Program Structure

The Corporate Ethics and Compliance Program (Program) is intended to demonstrate in the clearest possible terms the absolute commitment of VSP Global® (VSP) to the highest standards of ethics and compliance. That commitment permeates all levels of VSP. There is a Corporate Ethics and Compliance Officer and a Corporate Ethics and Compliance Committee. All members of these group(s) are prepared to support you in meeting the standards set forth in this Program.

The Corporate Ethics and Compliance Officer is:

- Dan Schauer, Global Corporate Finance and Risk Officer, VSP Global®

Members of the Corporate Ethics and Compliance Committee are:

- Dan Schauer, Global Corporate Finance and Risk Officer, VSP Global®, Corporate Ethics and Compliance Officer
- Alejandra Clyde, Sr. Manager, Office of General Counsel, VSP Global®
- Jeff DeRose, Director, Plexus Supply Chain, VSP Vision Care
- Rod Ehsani-Nategh, Vice President, Internal Audit, VSP Global®
- Lisa Fields, Vice President, Office of General Counsel, VSP Global®
- Maria Gregorio, Manager, Internal Audit, VSP Global®
- Melody Healy, Chief Strategy Officer, VSP Global®
- Hillary White-Nash, Sr. Compliance Specialist, Office of General Counsel, VSP Global®
- Gina Rosenberger, Vice President, Human Resources, VSP Global®
- Stuart Thompson, Vice President, Office of General Counsel, VSP Global®
- Guy Turner, Chief Information Security Officer, Global Technology Solutions, VSP Global®
- Jonathan Worrall, Vice President, Operations, Omni Channel Solutions
- Rob Winchell, Sr. Manager, Eyefinity, VSP Global®
- Thomas Fessler, Chief Legal Officer, serves as Legal Counsel to the Committee.

Resources for Guidance and Reporting Violations

To obtain guidance on an ethics or compliance issue or to report a suspected violation of this policy, you may choose from several options. VSP encourages resolution of issues at a local level whenever possible. If appropriate under the circumstances, first raise concerns with your onsite supervisor. If this is not appropriate under the circumstances, discuss your concerns with another member of management. u may also contact the confidential toll-free Ethics Reporting Hotline (The Network), at 1-877-349-7494 or the Office of the General Counsel (OGC) to report your concerns. The Network will submit the information to VSP's Ethics and Compliance Committee, which will immediately investigate all reports to the Hotline. The Network facilitates anonymous reporting for any caller who wishes to remain anonymous.

VSP will make every effort to maintain, within the limits of the law, the confidentiality of any individual who reports possible misconduct. There will be no retaliation for reporting a possible violation. Any Contingent Workers or Service Providers who deliberately makes a false accusation will be subject to discipline.

Personal Obligation to Report

We are committed to ethical and legal conduct that is compliant with all relevant laws and regulations and to correcting wrongdoing wherever it may occur in VSP. Each Contingent Workers or Service Providers has an individual responsibility for reporting any activity by any Contingent Workers or Service Providers, Contingent Workers or Service Providers, VSP doctor, group, or vendor that appears to violate applicable laws, rules, regulations, or this Code.

Investigations of Reports

VSP is committed to investigate all reported concerns promptly and confidentially to the extent possible. The Corporate Ethics and Compliance Officer or the Office of the General Counsel will instigate and coordinate all appropriate investigation(s) and immediately report and implement any corrective action(s) or change(s) that must be made. Contingent Workers or Service Providers must cooperate with VSP's investigation efforts.

XXIII. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law designed to protect health insurance coverage for individuals and their families. The law covers many aspects of healthcare, ranging from portability of health coverage from one job to another to the tax codes dealing with healthcare. Title II, Administrative Simplification, contains the provisions that will have the most significant impact upon VSP Global® (VSP). The Administrative Simplification provisions of the law affect healthcare providers, health plans, and healthcare information clearinghouses. The provisions seek to improve the efficiency and effectiveness of the healthcare system by:

- Standardizing the electronic data interchange (EDI) of many administrative and financial transactions; and
- Protecting the security and privacy of health information in electronic or paper formats.
-

Notice of Privacy Practices

A Notice of Privacy Practices is available to all VSP members on our website, http://www.vspglobal.com. In addition, members may contact VSP directly at 1-800-877-7195 to request a copy of our Notice. The Notice of Privacy Practices includes information about VSP's use and disclosure of protected health information for the purposes of treatment, payment and healthcare operations. The Notice also reviews the additional disclosures allowed by the law as well as describes the rights that a member has to their protected health information, including right to access, amend and request restriction. Lastly, the Notice provides VSP members with individual contact information for further information about privacy rights and protections as well as information on how to complain to the Secretary of Health and Human Services if they believe their privacy rights have been violated.

Compliance Responsibility

VSP has a team of individuals dedicated to ensuring HIPAA compliance. If you have specific questions about VSP's HIPAA compliance status, please e-mail your questions to hipaa@vsp.com.

Internal Audit and Other Monitoring

VSP monitors compliance with state and federal regulations and its policies. The Finance Department's Special Investigative Unit routinely conducts internal audits related to regulatory and compliance matters.

Information Confidentiality Classification Matrix for Service Provider

Note: "VSP" includes all VSP companies

	Public	Proprietary External	Proprietary Internal	Confidential
Description	Not sensitive; available to anyone	VSP owned; requires prior authorization for release outside of the Company	VSP owned; not to be disclosed or used outside of VSP	VSP owned; not to be disclosed or used beyond select internal or external audiences
Impact of Unauthorized Disclosure	Disclosure, use, or destruction of public information or data should have no adverse impacts on the organization or carry any liability	May adversely impact the organization; could undermine the confidence in and reputation of the organization	May seriously impact the organization; could jeopardize the organization's competitive edge; could undermine the confidence in, and reputation of, the organization	Would severely impact the entire system, individual persons, and the public; incur financial or legal liabilities; damage confidence in, and impair the reputation of, the organization
Possible Examples	vsp.com homepage content; readily available news and information posted on Globalview and vsp.com	Product offerings; Contingent Workers or Service Providers info for confidential surveys conducted by outside entities; Provider Reference Manual; underwriting rates; internal phone number listings; audited financial reports	Contingent Workers or Service Providers login IDs; VSP's third-party partner information; organization charts; Sales411 content; competitive data; doctor fees	Protected health information; doctor IDs; Contingent Workers or Service Providers personal information, e.g., SSN and payroll; client billing information; unaudited financial statements; budget-to- actual reports; Board minutes
Access	All	Available to Contingent Workers or Service Providers and approved Contingent Workers or Service Providers; requires prior authorization prior to disclosure outside of VSP	Available to Contingent Workers or Service Providers only; not for disclosure or use outside of VSP	Available to select Contingent Workers or Service Providers and authorized Contingent Workers or Service Providers with a nondisclosure agreement, granted on a need-to-know basis; an access list must be maintained
Handling	N/A	Same as Confidential, plus disclosure outside of VSP requires prior approval of division Vice President	Same as Confidential, plus do not disclose outside of VSP	Use secure-print or printer-mailbox function when printing; lock printed materials, discs, CDs, and DVDs in desk or cabinet when leaving work space; shred unneeded or unused printed material or place in marked secure waste bin; logout or lock computer screen when leaving desk; use encryption, e.g., Tumbleweed software, when e-mailing external information; remove or neutralize the magnetic field of discs before discarding; don't create databases containing confidential information or data without domain-owner approval; use standard templates and watermarks for printed material whenever possible

XXIV. VSP E-mail Retention Guidelines

Generally, e-mails are temporary communications that are vital and should be discarded routinely. However, depending on the content, the e-mail may be considered an official record of a transaction or discussion. Contingent Workers or Service Providers have the same responsibilities for e-mail messages and attachments as they do for any other company document or record, and must distinguish between vital and vital information.

The sender of the e-mail is responsible for ensuring proper retention of e-mails designated as vital and sent within VSP Global® (VSP). All other copies are duplicates and may be deleted. However, if an e-mail designated as vital was sent by someone outside VSP, the recipient is responsible for retention.

Retention Period

The period by which Electronic Communications must be kept or retained for later retrieval (Retention Period), is also determined by its content or purpose, as well as, by regulatory, statutory and archival history needs. The timeframe for retention or deletion can be found in VSP's Record Retention policy. When in doubt about the appropriate Retention Period, please contact the Office of the General Counsel at (800) 852-7600.

As a general practice, VSP automatically deletes Electronic Communications and attachments according to its Retention Guidelines. In order to preserve Electronic Communications past the retention guideline(s), Contingent Workers or Service Providers should either:

- Print the electronic communication and store the hard copy in a secured physical location; or
- Move the electronic communication into the appropriate Outlook folder designated to store contents indefinitely.

Each line of business shall determine which of the methods is appropriate for their area. Other storage locations, such as shared network drives, **must not be used**. All printed and electronic copies that must be kept beyond the Retention Period must be reviewed periodically to determine if there is still a business need for keeping it.