PEOPLE Related Company Policies

Below are the key PEOPLE related Company policies, which include policies that are issued at the time of employment and/or as part of the PEOPLE Department’s annual documentation audit.

It is very important to ensure awareness of the contents of these policies and ask either the Department Manager, a member of the PEOPLE Department, or the Chief Compliance Officer if any questions arise regarding the content of these policies.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Location</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate Behavior Policy</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Confidentiality Policy</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Equipment Usage – Code of Conduct</td>
<td>HR Manual</td>
<td>IT</td>
</tr>
<tr>
<td>Electronic Accounts – Policies of Use</td>
<td>HR Manual</td>
<td>IT</td>
</tr>
<tr>
<td>Inventions</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Payments of Gifts or Entertainment</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Press Statements</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Social Media Policy</td>
<td>HR Manual</td>
<td>IT</td>
</tr>
<tr>
<td>Drugs, Alcohol &amp; Weapons</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Dress Code</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>General Conduct Policies</td>
<td>HR Manual</td>
<td>PEOPLE</td>
</tr>
<tr>
<td>Vantage Code of Business Conduct &amp; Ethics</td>
<td>Vantage Website</td>
<td>Legal</td>
</tr>
<tr>
<td>Vantage FCPA Policy</td>
<td>Vantage Website</td>
<td>Legal</td>
</tr>
<tr>
<td>Vantage Whistleblower Policy</td>
<td>Vantage Website</td>
<td>Legal</td>
</tr>
<tr>
<td>Vantage FCPA Procedures</td>
<td>Vantage Website</td>
<td>Legal</td>
</tr>
</tbody>
</table>
17.1 INAPPROPRIATE BEHAVIOR POLICY

PURPOSE

The purpose of this policy is to develop a working environment in which inappropriate behavior, which includes bullying or harassment, is unacceptable and where Employees have the confidence to lodge a complaint against another Employee about any perceived harassment with the assurance that his or her concerns will be dealt with appropriately by the Company. Any complaints of inappropriate behavior will be handled by the PEOPLE Department and the immediate Department Manager.

SCOPE

This procedure applies to all Employees of the Company.

RESPONSIBILITY

Department Managers and Supervisors are responsible to ensure that no Employee is subjected to any form of inappropriate behavior, which includes but is not limited to harassment or bullying, and as is defined in this Policy and any known cases must be reported formally to the PEOPLE Department.

POLICY

The Company expressly prohibits and will not tolerate inappropriate behavior.

PROCEDURE

The Company expressly prohibits and will not tolerate any bullying, harassment or victimization of any kind including gender, race, color, religion, national origin, pregnancy, citizenship status, veteran’s status, age, genetic information or disability.

The Company believes that all Employees are entitled to be treated with dignity and respect while at work and when representing the business in any capacity outside of work. The purpose of this policy is to establish a working atmosphere that is free of harassment.

Company Prohibits all Inappropriate Behavior

Company considers all sexual conduct and comments, and conduct and comments that are sexual or are offensive on the basis of race, color, religion, national origin, sex, pregnancy, age, disability, veteran status, genetic information, sexual orientation, or any other characteristic or status protected by law, to constitute inappropriate behavior. Such inappropriate behavior is explicitly prohibited by this policy.
Company’s prohibition on inappropriate behavior is not limited to behavior that is actually severe or pervasive enough to constitute illegal discrimination or harassment. Rather, Company prohibits all behavior which is offensive on the basis of the characteristics and statuses described above, regardless of whether the behavior meets the legal definition of unlawful discrimination or harassment.

This policy also prohibits inappropriate behavior regardless of whether the inappropriate behavior is unwelcome, regardless of whether anyone has complained about the inappropriate behavior, and regardless of whether the person engaging in the inappropriate behavior intended for it to be offensive. This policy also prohibits inappropriate behavior which was intended only as a joke or was not supposed to be seen or overheard by others.

In other words, this policy prohibits all e-mails, jokes, letters, posters, screen savers, pictures, objects, propositions, conduct, comments, graphic displays, suggestions, advances, and physical touching which are sexual in nature or are offensive on the basis of race, color, religion, national origin, sex, pregnancy, age, disability, veteran status, genetic information, sexual orientation, or any other characteristic or status protected by law.

Company Prohibits Illegal Discrimination and Harassment

Company’s prohibition on inappropriate behavior includes a prohibition on discrimination and harassment that is actually illegal. Illegal discrimination and harassment includes discriminatory verbal or physical conduct which is unwelcome and which is made a term or condition of a person’s employment.

Illegal sexual harassment, for example, is defined as any unwelcome sexual advance, request for sexual favors, or other sexual conduct of a verbal or physical nature when:
1. Submission to such conduct is made either explicitly or implicitly a term or condition of a person’s employment;
2. Submission or rejection of such conduct by an individual is used as the basis for an employment decision affecting that person; or
3. Such conduct has the purpose or effect of unreasonably interfering with an individual’s work performance or creating an intimidating, hostile or offensive working environment.

No Manager or other Employee shall threaten or insinuate that another Employee’s or applicant’s refusal to submit to sexual advances will adversely affect any aspect of that person’s employment. No Manager or Employee shall promise, imply, or grant any preferential treatment to another Employee or applicant in exchange for engaging in sexual conduct. No Manager or other Employee shall engage in any inappropriate behavior which has the purpose or effect of unreasonably interfering with an Employee’s work performance or creating an intimidating, hostile, or offensive working environment.
Company Prohibits Retaliation

Under no circumstances will an Employee who in good faith reports alleged incidents of illegal discrimination, harassment, or other inappropriate behavior, or who cooperates in an investigation of any such report, be subjected to any form of reprisal or retaliation on account of his/her report or cooperation in such an investigation. Any Employee who feels that he/she has been retaliated against or threatened with retaliation should immediately report the retaliation or threat to his/her Manager or the Director of HR.

Employees Have Rights and Responsibilities

Employees Have The Right To Speak Up. Employees who feel that they have been subjected to discrimination, harassment, other inappropriate behavior, or retaliation should remember they have the right to speak up and tell the person or persons responsible that their conduct is unwelcome, offensive, and inappropriate. Whether or not the Employee chooses to let others know their behavior is unwelcome and offensive, the Employee should report the matter to the PEOPLE Department immediately.

Report All Inappropriate Behavior And Retaliation. Any Employee who feels that he/she has been a victim of any type of discrimination, harassment, other inappropriate behavior, or retaliation should immediately contact his/her Manager or the Director of HR. Likewise, an Employee who witnesses discrimination, harassment, other inappropriate behavior, or retaliation should immediately report it to the Director of HR.

Be Prompt. Prompt reports are important; they help Company eradicate discrimination, harassment, other inappropriate behavior, and retaliation and facilitate prompt and thorough investigations. For this reason, an Employee should always make a report as soon as possible, usually within 24 hours. Employees should not wait for a situation to become worse or unbearable before making a report. If, for example, a Manager makes inappropriate sexual comments, the Employee should not wait until the comments interfere with his or her ability to do the job. Instead, the Employee should contact the Director of HR. Even if an Employee does not report the discrimination, harassment, or inappropriate behavior within 24 hours, the Company still wants the Employee to report the matter and Company will still deal with the matter promptly.

Company Will Investigate

All reports of discrimination, harassment, other inappropriate behavior, and retaliation will be taken seriously and will be investigated promptly. To the extent possible, the Company will keep the identity of the reporting Employee confidential. However, under certain circumstances, the Company may need to disclose the reporting Employee’s identity as part of the investigation itself (for example, to provide an opportunity to respond to the complaint). The Company will not tolerate retaliation in any form against an Employee who makes a report of illegal discrimination, harassment, other inappropriate behavior, or retaliation. Any Employee who, after an investigation, is determined to have engaged in any form of discrimination, harassment,
Inappropriate Behavior Policy

other inappropriate behavior, or retaliation will be subject to appropriate disciplinary action, up to and including discharge.

While the Company is committed to preventing and correcting unlawful discrimination, harassment, other inappropriate behavior, and retaliation, it also recognizes that false accusations may harm the innocent party who is falsely accused. Accordingly, any Employee who, after an investigation, is found to have knowingly made a false accusation of discrimination, harassment, other inappropriate conduct, or retaliation may be subject to appropriate disciplinary action. However, if an Employee makes a report of what he/she in good faith believes to be discrimination, harassment, other inappropriate behavior, or retaliation, the Employee will not be subjected to disciplinary action, even if the Employee turns out to have been mistaken.

DOCUMENTATION

N/A
17.2 CONFIDENTIALITY POLICY

PURPOSE

As part of the Employee’s employment with the Company, an Employee will be provided with and exposed to certain written and oral information that is non-public, confidential and proprietary in nature respecting the Company, its business and operations. The purpose of this Policy is to make Employees aware of the limitations and expectations surrounding such access to this information.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

The Company expressly prohibits and will not tolerate breach of confidentiality or any other unlawful activity.

PROCEDURE

Trade Secrets and Confidential Information

(a) All Employees must acknowledge, understand and agree that all Confidential Information, as such term is defined below, whether developed by Employee or the Company, is the exclusive and confidential property of the Company and shall be regarded, treated and protected as such in accordance with this Policy. Employee acknowledges that all such Confidential Information is in the nature of a trade secret. Failure to mark any writing confidential shall not affect the confidential nature of such writing or the information contained therein.

“Confidential Information” means oral or written information, which is used in the business of the Company and (i) is proprietary to, about or created by the Company, (ii) gives the Company some competitive business advantage or the opportunity of obtaining such advantage or the disclosure of which could be detrimental to the interests of the Company, (iii) is designated as Confidential Information by the Company, is known by Employee to be confidential and proprietary to the Company, or (iv) is not generally known by non-Company personnel. Such Confidential Information includes, without limitation, the following types of information and other information of a similar nature (whether or not reduced to writing or designated as confidential): (i) information related to all proprietary information developed, licensed or otherwise acquired by the Company, (ii) internal
personnel and financial information of the Company, vendor information (including vendor characteristics, services, prices, lists and agreements), purchasing and internal cost information, internal service and operational manuals, data bases, computer software, and the manner and methods of conducting the business of the Company, (iii) marketing and development plans, price and cost data, price and fee amounts, pricing and billing policies, quoting procedures, marketing techniques, forecasts and forecast assumptions and volumes, and future plans and potential strategies (including, without limitation, all information relating to any acquisition prospect and the identity of any key contact within the organization of any acquisition prospect) of the Company which have been or are being discussed, (iv) names of customers, suppliers and their representatives, contracts (including their contents and parties), customer services, and the type, quantity, specifications and content of products and services purchased, leased, licensed or received by customers or suppliers of the Company, and (v) confidential and proprietary information provided to the Company by any actual or potential customer, supplier, government agency or other third party (including businesses, consultants and other entities and individuals).

(b) Notwithstanding anything to the contrary, the provisions of this Section 1 shall not apply to information that: (i) was, is now, or becomes generally available to the public (but not as result of a breach of any duty of confidentiality by which Employee is bound); (ii) was disclosed to Employee by a third party not subject to any duty of confidentiality to the Company prior to its disclosure to Employee; or; (iii) was disclosed by Employee in the ordinary course of the Company’s business as a proper part of Employee’s duties in connection with communications with customers, vendors and other proper parties, provided that it is for a proper purpose solely for the benefit of the Company.

(c) Employee will occupy a position of trust and confidence with respect to the affairs and business of the Company. In view of the foregoing, Employee agrees that it is reasonable and necessary that Employee make each of the following covenants: (i) Employee shall not disclose Confidential Information to any person or entity, either inside or outside of the Company, other than as necessary in carrying out Employee’s duties and responsibility in service to the Company, without first obtaining the Company’s prior written consent (unless such disclosure is compelled pursuant to court orders or subpoena, and at which time the Employee shall give prior written notice of such proceedings to the Company); (ii) Employee shall not use, copy or transfer Confidential Information other than as necessary in carrying out Employee’s duties and responsibility in service to the Company, without first obtaining the Company’s prior written consent; (iii) Employee shall not make any statement or disclosure that would be prohibited by applicable laws, or is intended or reasonably likely to be detrimental to the Company or any of its subsidiaries or affiliates; and -

(d) Employee will occupy a position of trust and confidence with respect to the affairs and business of the Company. In view of the foregoing, Employee agrees that it is reasonable and necessary that Employee make each of the following covenants: (i) Employee shall not disclose Confidential Information to any person or entity, either inside or outside of the Company, other than as necessary in carrying out Employee’s duties and responsibility in service to the Company, without first obtaining the Company’s prior written consent (unless such disclosure is compelled pursuant to court orders or subpoena, and at which time the Employee shall give prior written notice of such proceedings to the Company); (ii) Employee shall not use, copy or transfer Confidential Information other than as necessary in carrying out Employee’s duties and responsibility in service to the Company, without first obtaining the Company’s prior

If printed, this document is regarded as "uncontrolled"
written consent; (iii) Employee shall not make any statement or disclosure that would be prohibited by applicable laws, or is intended or reasonably likely to be detrimental to the Company or any of its subsidiaries or affiliates; and (iv) at the conclusion of Employee’s employment with the Company, Employee shall promptly deliver to the Company (or its designee) all written materials, records and documents made by the Employee or which came into Employee’s possession during the term of Employee’s employment with the Company concerning the business or affairs of the Company, including but not limited to keys, laptops, thumb drives, flash drives, USB drives, cell phones, credit cards, access badges, Company documents, and electronic information and without limitation, all materials containing Confidential Information. If Company information is stored on a device owned by the Employee (e.g., a computer or USB drive), the Employee must notify the IT Department so that arrangements may be made to return the information and remove it from the Employee’s device.

Miscellaneous

(a) Equitable Relief. Employee acknowledges that any violation or threatened violation of this Policy shall cause irreparable injury to the Company and that, without prejudice to the rights and remedies otherwise available, the Company shall be entitled to equitable relief by way of injunction if Employee breaches or threatens to breach any of the provisions of this Policy.

(b) Amendment and Waiver. The provisions of this Policy may be amended or waived only in writing with the prior written consent of the Company, and no course of conduct or course of dealing or failure or delay by any party hereto in enforcing or exercising any of the provisions of this Policy shall affect the validity, binding effect or enforceability of this Policy or be deemed to be an implied waiver of any provision of this Policy.

(c) Severability. Whenever possible, each provision of this Policy shall be interpreted in such manner as to be effective and valid under applicable law, but if any provision of this Policy is held to be invalid, illegal or unenforceable in any respect under any applicable law or rule in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other provision of this Policy or any action in any other jurisdiction, rather instead this Policy shall be reformed, construed and enforced in such jurisdiction as if such invalid, illegal or unenforceable provision had never been contained herein.

(d) Assignment. This Policy shall be binding upon and inure to the benefit of the Company and its respective successors, legal representatives and assigns, and upon the Employee, Employee’s heirs, executors, administrators, representatives and assigns.

(e) Entire Agreement; No Oral Amendments. This Policy constitutes the entire agreement between the Company and Employee with respect to the subject matter of this Policy.

(f) Choice of Law. THIS POLICY SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, WITHOUT REGARD TO THE PRINCIPLES OF CONFLICTS OF LAW.
(g) Title and Headings; Construction. Titles and headings to Sections hereof are for the purpose of reference only and shall in no way limit, define or otherwise affect the provisions hereof.

(h) No Strict Construction. Employee represents to the Company that Employee is knowledgeable and sophisticated as to business matters, including the subject matter of this Policy, that Employee has read the Agreement and understands its terms and conditions. The parties hereto agree that the language used in this Policy shall be deemed to be the language chosen by them to express their mutual intent, and no rule of strict construction shall be applied against either party hereto. Employee acknowledges that Employee has had the opportunity to consult with counsel of Employee’s choosing, independent of the counsel for the Company, regarding the terms and conditions of this Policy and has done so to the extent that Employee, in Employee’s sole discretion, deemed to be appropriate.

(i) Counterparts. This Policy may be executed and delivered (including by facsimile or Portable Document Format (pdf) transmission) in any number of counterparts with the same effect as if all parties hereto had signed the same document. Facsimile and other electronic copies of manually-signed originals shall have the same effect as manually-signed originals and shall be binding on all parties hereto. All counterparts must be construed together to constitute one and the same instrument.

DOCUMENTATION

N/A
17.3 ELECTRONIC ACCOUNTS POLICY

PURPOSE

The purpose of this policy is to establish standards for privacy, confidentiality, and security for electronic accounts and to ensure they are used for purposes appropriate to the Company, are in compliance with applicable laws, and to prevent disruptions and misuse.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

The Company defines that Vantage Employees need to be aware of the potential risks to the Company and themselves through electronic accounts.

PROCEDURE

The use of electronics for information and communications can generate a number of issues. It is important that Vantage Employees are aware of Company policy, the potential risks to the Company and themselves, their obligations, and means of protection.

1. Facilities for electronic communications are Company systems and are provided for Company use.
2. Vantage Employees have an obligation to comply with all Company policy and standards. Vantage Employees are expected to maintain the Company’s high ethical standards and to adhere to standards relating to the external representation of the Company. Official correspondence, transmitted electronically, must comply with Corporate and Divisional standards.
3. Vantage Employees are considered to be representing the Company in any electronic communications, and as such the content and language used should be consistent with that used for official correspondence. Care must be taken to protect Company reputation in all communications, official or unofficial (e.g. Vantage Employees must be careful not to defame or be critical of persons in other organizations). Vantage Employees should note that the use of electronic communications enables recipients to easily use the contents for purposes not originally intended (e.g. forwarding to unintended recipients, copying, quotations).
4. Disclaimers may be used to distinguish professional opinion from official Company policy (i.e. the professional opinion of a Staff member). Purely personal opinions and feelings must not be expressed via Company communications facilities (even with a disclaimer) as the systems typically identify the Company and hence associate the person and the opinion or sentiment with the Company.
5. Material must be non-defamatory and non-discriminatory. Material offensive to groups or individuals is not permitted on Company systems in any form, permanent or temporary (e.g. racist, sexist or pornographic material).

6. Vantage Employees must observe copyright laws when sending, accessing, copying or printing material (documents, images, all forms of software, shareware, etc.). Accessible material may be subject to copyright or licensing conditions. All reasonable steps must be made to ascertain and comply with applicable conditions.

7. Vantage Employees must be aware of and comply with any contractual obligations and/or applicable local laws. Vantage Employees must be aware of the local laws pertaining to trade practices or anti-trust. Any queries or doubts should be checked with the Legal Division and Management. Local customs are to be observed providing they do not conflict with Company policy.

8. Vantage Employees should note that the Company may or may not indemnify Vantage Employees against breaches of certain types of legislation, and that in some instances the Company may have to take action against a member of Staff for breaches of a particular piece of legislation. Vantage Employees should be aware that they may be held personally liable for any such breaches.

9. All software downloaded electronically must be licensed for Company use, checked for viruses, and comply with Company and Divisional standards.

10. Vantage Employees who, for whatever reason, may be privy to confidential information are bound by Company policy and by applicable statutory legislation relating to privacy, copyright, and misuse of Company assets. Vantage Employees must also be aware that electronic communication frequently transverses third party networks and mail systems, and may be monitored there for support or other purposes.

11. Vantage Employees are responsible for correctly addressing mail messages, and should take care when addressing mail, as mail directories include many similar names as well as external parties.

12. Employees must understand that electronic communications may not be private and may be reviewed by, among others, the Company, other Company Employees, or the providers of any communications service.

13. Vantage Employees using any Company electronic communications system must be identifiable (e.g. via allocation of equipment, extensions or user-id's). Anonymous use of Company electronic information or communication systems is not allowed.

14. The contents of all electronic information and communications using Company equipment are considered to be Company records and must be treated accordingly. The Company may access and disclose electronic information and messages sent via electronic communication. Access and disclosure will be for legitimate purposes only and is subject to Legal Department and Management approval. The Company will not monitor electronic communication messages as a routine matter.

15. Vantage Employees have an obligation to protect Company information and intellectual property. Vantage Employees' knowledge of Company operations, procedures, technologies etc. is part of Company intellectual property and is integral to the Company's competitive advantage. Vantage Employees should be aware of the value of their knowledge and must take appropriate steps to protect this asset.
16. Vantage Employees should be aware that there are significant costs associated with the provision of electronic communication systems and services. None of the services are free. Vantage Employees should expect to be able to explain their usage of facilities, and the costs and benefits to the Company.

17. Limited personal use may be tolerated at the discretion of the Employee’s Manager. Significant personal use is not permitted. The definition of "Significant Use" is solely at the discretion of Management.

18. Vantage Employees using Company systems and facilities for personal use must comply with all Company policy, legal and contractual obligations.

19. Any personal use should be noted as personal within the content of the communication and should not reference the Company nor use Company stationery.

20. Non-Company use by contractors or temporary Vantage Employees will be treated as personal use.

21. Vantage Employees are responsible for security of their electronic accounts. Vantage Employees must not disclose or share account passwords with others. It is essential that passwords are protected, and are set and changed in accordance with Company Information Technology standards.

22. In cases where authentication of electronic communication is important, the sender and recipient(s) should confirm the transaction via non-electronic means.

23. Temporary accounts are available for temporary Staff who may work in a permanent Staff member's place from time to time. Permanent Vantage Employees must have their own account names and passwords.

24. Vantage Employees must not use electronic communication systems (voice mail / e-mail) as a permanent storage of messages. Electronic communication messages to be retained on a longer term basis must be filed within the departmental filing system (paper or electronic).

25. Messages relating to the substantive business of the department, containing a formal communication, or which have continuing value, should be filed. Where possible Vantage Employees should identify the relevant file reference on the mail message.

26. Transitory messages of minor importance and "copies" of messages distributed to a number of Vantage Employees should be deleted from the electronic communication system as soon as the need for them ceases.

27. Storage and retention of all Company records, electronic or paper, should be in accordance with normal departmental procedures and Company Information Technology standards.

28. Vantage Employees should be aware that electronic communication messages marked by them for deletion might still be held on the system for a period of time. Similarly, other recipients may have stored copies of messages deleted by them. Note also that messages may be received, read, and deleted, and not be recorded on a backup system.

29. Backups of mail systems are required for system recovery purposes only and are not appropriate for permanent storage or archival of messages. Therefore, Vantage Employees should not make routine requests for retrieval of electronic communications from backup media. It will not be practical to recover electronic communication messages recently deleted or marked for deletion from system backup media.

30. Vantage Employees should log off their computers at the end of the day or when leaving machines unattended for long periods of time. Turning off the computer is not required, only logging off.
31. Vantage Employees must keep all files in the network directories provided so that computer administrators can maintain regular backups.
32. Vantage Employees choosing to keep files on their individual hard drives accept responsibility for the potential loss of those files. Computer administrators may be required to erase and rebuild hard drive partitions, or files may be lost due to hard drive failure. Computer administrators cannot recover files lost from local drives.
33. Vantage Employees must not disable virus scanning.
34. Vantage Employees must not make copies of software or install software to any number of machines without a separate, appropriate license for each machine you install the software to. The penalties for breaking this rule can be severe, as software piracy is against the law.
35. Any doubts regarding use of electronic information and communication services should be cleared with the Employee’s Manager.

DOCUMENTATION

N/A
17.4 ELECTRONIC EQUIPMENT USAGE – CODE OF CONDUCT

PURPOSE

To establish a consistent set of computing security practices for Vantage users who use personal devices in conjunction with the performance of work activities and maintenance.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

Employees are obliged to take every possible precaution to ensure that data is only available to those authorized to see and or use it.

PROCEDURE

Personal Computers

Vantage issues standardized PCs to all Employees. Not all Employees are allowed to use personal devices in the workplace or in the performance of their duties. Therefore Employees who are permitted and choose to use personal devices are responsible to comply with the guidelines in this policy. That means that the burden of maintaining an Employee’s personal device or computer and ensuring that it is secure falls to each Employee. Vantage expects that the following measures will be taken by each Employee where appropriate:

1. Operating System updates (especially security updates) will be applied in a timely manner.
2. Anti-virus software will be installed and used where available and appropriate.
3. Reasonable care will be taken when visiting web sites, downloading unknown software, etc.
4. Your Operating System will be configured to require a password on power-up and wake from sleep.

Portable Computers

Employees are expected to take reasonable care to secure any computer that might contain Company or customer data, but special care should be taken with portable computing devices (e.g. laptops or smartphones). Any private data on a portable device should be stored only in encrypted form, a password should be required for access and only encrypted channels should be used for checking email, transferring files, collaboration, screen-sharing, etc. (e.g. you must use https or SSL for email via a public wireless network).
PGP Whole Disk Encryption is available Mac OS X and Windows and provides a very easy to use solution for ensuring that all private data is encrypted on your laptop. Upon installation, it encrypts the entire hard disk, ensuring that databases, sensitive emails, spreadsheets, etc. are all protected regardless of where they’re stored on the computer. If the laptop is ever stolen, the thief will have no access to anything on the disk and have to reformat to even use the computer.

**Passwords**

Employees are expected to take reasonable care to use effective passwords for any accounts, computers, etc. that might allow access to sensitive customer, member or Company data. Passwords should be safeguarded and changed regularly. When you have access to shared passwords (admin, guest accounts, etc.) you are expected to take special care to safeguard the passwords and never expose them to others.

**Data Security**

Any confidential Company or customer data will be stored on physically secure computers or will be encrypted when on portable devices or backup tapes, DVDs, etc.

All transfer of Vantage data over the Internet must be encrypted. Checking and sending email, transferring files, etc. should be done via a secure channel (e.g. SSL), especially when using third-party or wireless networks.

Any printouts or faxes of customer or Company sensitive data should be under secure control at all times and destroyed when no longer needed.

**Security Violation Reporting**

In the event that a security violation occurs, (network breach, lost/stolen laptop, intercepted email, etc.) the event must be reported to the IT Department immediately.

**DOCUMENTATION**

N/A
17.5 INVENTIONS POLICY

PURPOSE

To summarize Employees’ responsibilities as they relate to inventions.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

All work-related inventions during employment must be reported to the Chief Compliance Officer.

PROCEDURE

Any invention, copyright works, or designs made by an Employee in the normal course of employment at work will (as provided for in legislation) automatically become the property of the Company, unless otherwise agreed in advance in writing by both parties.

Any Employee who has created, designed, invented or otherwise; a new product, system, design etc. will not be eligible to claim copyright or ownership of such an item.

All Employees are responsible to notify his or her Department Manager, Rig /Country Manager and Supervisor if he or she has any issues relating to this policy.

DOCUMENTATION

N/A
17.6 PAYMENT OF GIFTS OR ENTERTAINMENT

PURPOSE

To establish guidelines that will help ensure compliance with laws and legislation that protect Employees.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

The Company and ALL its Employees should uphold the highest levels of honesty, integrity, ethical standards, and compliance with the law and to avoid actual or apparent conflicts of interest between his/her personal and professional affairs. No gifts should be given or received by any Employee and no entertainment should be extended or received if it could be considered to be extravagant.

PROCEDURE

In accordance with the Foreign Corrupt Practices Act (FCPA) and the Code of Business Conduct & Ethics, Employees are not permitted to make or receive payments or gifts from any contractor, supplier or other Company or person with whom the Company might have a contractual relationship.

Employees must seek advice from his/her Department Manager if he/she is uncertain about any aspect contained within any of these policies. All Employees should be familiar with the relevant Company documents that cover this.

Employees are encouraged to report any Employee who he/she believes might be breaching any of these policies. Please refer to the Whistleblower Policy.

Additional information can be found on the Vantage website under Corporate Governance and is translated into other languages.
Payment of Gifts or Entertainment

DOCUMENTATION

FCPA Policy

Code of Business Conduct and Ethics

Whistle-Blower Policy
17.7 PRESS STATEMENTS

PURPOSE

To ensure the correct channels of communication are followed when there might be media attention so that the Company can safeguard that information being released for public knowledge is accurate and appropriate at the time of release.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

Company Employees are not permitted to knowingly communicate with the Media in regard to Company business, operations, or actions taken by the Company.

PROCEDURE

Employees should not under any circumstance deal directly or indirectly with the press or other media related Company, individual, representative or otherwise, regarding any Company and/or Client related business. Media includes contact with a member from Radio, Television, Magazines, Newspapers, and Internet etc.

In cases where an Employee has been contacted (or is in contact) with a member of the media, he or she must direct the caller immediately to his or her Department Manager or alternatively directly to the Company’s Legal Department in Houston. If this is not practical, then the receiver of the call (a call might be in person or via telephone etc.) should take a message. Under no circumstances should the receiver have any dialogue with the Media other than to take a message.

Relevant contact details can be found in Guidance Note 24 – Vantage Offices & Country Specific Information. Similarly Employees are not permitted to provide to the media copies of letters, emails or articles regarding any aspect of the Company and/or its Client’s business, unless first having obtained written permission from an Executive Officer of the Company.

Department Managers, Rig/Country Managers and supervisors are responsible to ensure Employees are aware of the procedure to follow in the event that he or she is contacted by any member of the Media.
DOCUMENTATION

Guidance Note 24 – Vantage Offices & Country Specific Information
17.8 SOCIAL MEDIA POLICY

PURPOSE
To establish protocol for appropriate and inappropriate behaviors as it relates to the workplace when it comes to the use of social media and to provide general guidelines for Employees on workplace access and appropriate usage of social and professional networking sites.

SCOPE
This policy applies to all Employees, contractors, business partners, and/or other parties representing the Company referred to here as “associates”.

RESPONSIBILITY
It is the responsibility of all Employees of the Company to adhere to this policy and for reading, knowing, and complying with the Terms or Use of the social media sites they use.

It is the responsibility of Department Managers to ensure that any contractors, business partners or other parties receive a copy of this policy.

POLICY
Employee communications, whether written, oral or through social media, must at all times comply with Vantage’s Code of Business Conduct and Ethics and Vantage’s Electronic Services Accounts: Policies of Use.

PROCEDURE
State of Social Media
Vantage recognizes that social media, professional networking sites, rapid-fire communications, blog sites, and personal Web sites are all useful technologies. Every associate has an opportunity to express and communicate online in many ways, and Vantage respects the appropriate uses of an associate’s online presence. Above all else, every associate needs to use good judgment on what material makes its way online.

Associates take full responsibility for any content presented in social media and shall indemnify and hold harmless Vantage against claims or damages resulting from their participation in social media.

This policy will set forth guidelines that Employees should follow for all online communications in reference to Vantage.
Relevant Technologies

This policy includes (but is not limited to) the following specific technologies:

- Personal and public blogs
- LinkedIn
- Twitter
- Facebook
- MySpace
- Personal Web sites
- Flicker
- Youtube
- Digg

Topic Matter Guidelines

Vantage Employees are to use the following guidelines in social networking practices:

- Restrict content to matters not related to Vantage or its business. Disclosure or discussion regarding Vantage is expressly prohibited.
- Do not be anonymous.
- Maintain professionalism, honesty, and respect.
- Apply a "good judgment" test for every activity: Could you be guilty of leaking information, trade secrets, customer data, or upcoming announcements? Is it negative commentary regarding another associate or organization? A good judgment test is to ask yourself “would I, be or cause, embarrassment if what I did appeared on the front page of a newspaper?”
- Comply with the law in regard to copyright/plagiarism.
- Seek guidance from management when uncertain.

Activity showing good judgment would include statements of fact about Vantage and its services, facts about already-public information, or information on Vantage Web site.

If any Employee becomes aware of social networking activity that would be deemed distasteful or fail the good judgment test, please contact the anonymous social media response center at https://vantage.alertline.com

Company Assets

The use of Company assets (computers, Internet access, email, etc.) is intended for purposes relevant to the responsibility assigned to each Employee. Social networking sites are not deemed a requirement for most positions, and certain job titles are not permitted to access these services over the Internet. For Employees who are allowed to access these services, a reasonable and limited amount of use of Company assets are permitted for social networking services. Social media activities are not to interfere with the Employee’s primary job responsibility.

Inaccurate or Defamatory Content

Associates who participate in online communication will be subject to disciplinary action. This online communication can include, but is not limited to:

- Company information or data leakage.
- Inaccurate, distasteful, or defamatory commentary about the Company, an Employee or another organization.
Disciplinary action can include termination or other intervention deemed appropriate by The PEOPLE Department Resources.

**Restricted Material**
This policy sets forth the following items which are deemed restricted for social networking:

**Intellectual Property, Trade Secrets, or Customer Data**
Vantage's intellectual property, trade secrets, and customer data are strictly forbidden from any online discourse except through mechanisms managed internally by Vantage communications or marketing groups.

**Online Recommendations**
Some sites, such as LinkedIn, allow members to "recommend" current or former co-workers. Vantage forbids Employees to participate in Employee recommendations for reasons of Company liability. All communication of this type should be referred to the PEOPLE Department for verification.

**Financial Information**
Any online communication regarding the Company's financial data is strictly forbidden except through mechanisms managed internally by Vantage communications or marketing groups.

**Company-Sensitive Matters**
Any online communication regarding proprietary information such as strategic decisions, or other announcements deemed inappropriate for uncoordinated public exchange is forbidden.

**DOCUMENTATION**

N/A
17.9 DRUGS, ALCOHOL & WEAPONS

PURPOSE

To establish and maintain a safe, healthy working environment conducive to high levels of work performance for all Employees and visitors of any Company facility.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

OIM/ARM, Shore Based Facilities Managers, and Department Managers are responsible to ensure resources are in place to satisfy this Policy & Procedure and to conduct searches and screening as deemed necessary.

The VP QHSE is responsible to implement random screening requirements for drugs and alcohol as deemed necessary.

The Director of HR is responsible to implement pre-employment screening for drugs and alcohol as deemed necessary.

POLICY

The unauthorized use, possession, sale, purchase or distribution of any drugs, alcohol, weapons or any other controlled substances that violates any laws is strictly prohibited. While the Company has no intention of intruding in the private lives of Employees, the Company does expect Employees to report for work in a condition suitable for performing their duties. Drugs and/or Alcohol involvement, whether it is at work or at home, can pose serious risks.

PROCEDURE

Investigations & Searches

The Company reserves the right to conduct random searches as and when it deems necessary. These random searches can include all personnel and their personal effects including but not limited to clothing, baggage, toolboxes, lockers, or living quarters.
The Company reserves the right to conduct selective searches in situations where they deem there to be any reasonable belief, suspicion, or cause for concern that this policy could be in breach by any individual or group of individuals.

**Employment Screening**

As part of the recruitment procedure, the Company requires urinalysis, blood test, or other drug/alcohol screening of all Employees prior to full acceptance of any Formal Offer of Employment.

An Employee’s consent to submit to such a test is required as a condition of employment, and an Employee’s refusal to consent shall result in the offer of employment being withdrawn.

**Random Testing**

The Company reserves the right to subject personnel to random drug and/or alcohol screening/testing procedures. These may include urinalysis, blood test, or other. An Employee’s consent to submit to such a test is a condition of employment, and an Employee’s refusal to consent is a refusal to cooperate with the Company Policies & Procedures and constitutes gross misconduct which may result in disciplinary action up to and including summary dismissal.

In addition to random testing, below are typical examples of situations in which such tests may also be required:

- Accident investigations.
- Unexplained significant deterioration in individual job performance.
- Significant change in individual personality (e.g. abusive behavior, insubordination, etc.).
- Reports by others of individual or group drug or alcohol use where there is reason to believe there may be a violation of this policy.
- Unexplained absences from normal work sites where there is reason to suspect drug and/or alcohol related activity in violation of this procedure.
- Follow up testing for Employees who have failed the drug and/or alcohol tests previously.

**Disclosure**

When traveling to an offshore installation, Employees are required to report all medications to the Medic upon arrival. Failure to do so will result in disciplinary action being taken against the Employee, which may include up to Summary Dismissal from the Company. Additionally, when Employees are attending a Company Medical, they are required to disclose all medications to the examining doctor. Again, failure to disclose all medications, even if the medications are not consumed offshore at work, will result in disciplinary action being taken against the Employee, which may include up to Summary Dismissal from the Company.
Detection of Legal Drugs

Where use of a legal drug is detected, personnel may be required to offer proof that the drug has been prescribed to them by a medical professional. If the person is unable to provide such proof, appropriate action may be taken by the Company. For an Employee, this may include disciplinary action up to and including Summary Dismissal.

Employment may be denied, in accordance with applicable laws concerning disabled persons, where the use of the drug would impair job performance.

Release of Information

As a condition of employment, all Employees are required to agree to the release of all substance screens, reports and any associated documentation.

Controlled Substances/Legal Drugs or drugs that might affect performance/safety (e.g. cause vision impairment, drowsiness, sloppiness etc.) Personnel in possession of these Controlled Substances/Legal Drugs or drugs that might affect performance/safety shall report these to:

- Onshore Personnel – to their Manager/Supervisor or Company Medical Adviser.
- Offshore Personnel – to the Company Medical Adviser or PEOPLE Department prior to starting to travel to work and to the Offshore Medic immediately upon arrival on-board.

All prescription medications when reported to the Installation Medic shall be recorded on a Personal Medical Record HSE-27.

Prohibited Activities

On-board all offshore installations and at Company operated facilities, the following activities are strictly prohibited:

- Unauthorized possession, sale, distribution or use of weapons including but not limited to firearms, explosives, knives, axes, crossbows, or homemade implements.
- Possession, sale, distribution or use of alcohol.
- Being under the influence of alcohol.
- Use or possession of any drug or controlled substance that violate any law.
Disciplinary Actions

Any Company Employee or contracted personnel found in breach of this policy, or refusing to cooperate in any search or screening requirements, shall be subject to removal from the workplace and disciplinary action shall be taken as considered necessary by the Company.

Consequences of Failing Drug and/or Alcohol Screening

Employees who have been referred for urinalysis drug and/or alcohol screening shall be suspended without pay immediately. In the absence of compelling reasons for a positive result, such personnel shall be removed from the workplace and disciplinary action as considered necessary by the Company. Disciplinary action as a result of any breach of this policy can be severe including up to summary dismissal for the first violation at the sole discretion of the Company.

DOCUMENTATION

Guidance Note 08 – Drug and Alcohol Screening

Personal Medical Record HSE-27
17.10 DRESS CODE

PURPOSE

To provide guidelines for acceptable work attire so to ensure a professional appearance at all times.

SCOPE

This policy applies to all Employees of the Company.

RESPONSIBILITY

It is the responsibility of all Employees of the Company to adhere to this policy.

Department Managers are responsible to ensure his/her Employees dress appropriately while at work or while representing the Company.

POLICY

All Employees of the Company shall dress in a manner which is appropriate for the work and the location at which they are employed or visiting.

PROCEDURE

As the nature of each Employee’s work is widely varied throughout the Company, a formal dress code for Employees is not needed; however, for onshore Employees (or offshore Employees working onshore), the Company’s overall preference is that ‘business casual’ is the appropriate attire for most Employees. Any questions regarding the appropriateness of attire should be addressed to the PEOPLE Department.

There is no formal dress code for Employees working in shipyard/offshore locations; however, Employees must adhere to the (PPE) Personal Protective Equipment requirements at all times.

Casual Day – Onshore Office Locations

Fridays and Public Holidays are considered casual days whereby a more relaxed dress code is acceptable. Employees are requested to consider what meetings he/she may be attending and dress accordingly.

DOCUMENTATION

N/A
17.11 GENERAL CONDUCT POLICIES

PURPOSE
To ensure orderly operations and provide the best possible work environment.

SCOPE
This policy applies to all Employees of the Company.

RESPONSIBILITY
It is the responsibility of all Employees of the Company to adhere to this policy.

POLICY

Open Plan Policy
When working in an open plan environment, Employees are encouraged to be mindful of their colleagues. Noise should be kept to a minimum. Where any noise could be considered to be disruptive to other colleagues, headphone use is encouraged. The Company will provide you with headphones if requested. Employees who are seated in cubicles should not use the “loudspeaker” function on their phones, desktop, mobile, or otherwise. Additionally, Employees in offices are encouraged to close their doors when using the “loudspeaker” function on their phones.

Use of Phone, Postal and Courier Systems
In addition to what has been stated above, Employees should also practice discretion when making personal calls. Private offices can be made available should Employees need to make any confidential calls. The Company may request Employees to reimburse the Company for any personal calls that the Company considers to be excessive on Company provided telephones.

The use of the Company paid postage for personal correspondence is not permitted. Should an Employee need to use a courier for personal use then he/she must inform the Payroll Department to action the appropriate salary deduction from the Employee’s next salary or expense payment.

Attendance and Punctuality
Regular attendance and punctuality are conditions of employment. The Company recognizes that occasionally absence due to illness or emergencies is necessary and often beyond the control of an Employee. In such cases, the Company asks that Employees notify his/her Immediate Supervisor as soon as possible. Excessive absence and habitual tardiness are not acceptable and will be handled under the Company’s Disciplinary Policy and Procedure within the HR Manual.
Client Request to Remove an Employee from an Installation

As a condition of contract, the Client may have the contractual right to formally request, with cause, an Employee to be removed from a particular installation or to refuse to accept a particular Employee as a member of the offshore crew for a particular installation. The Company will handle such requests on a case by case basis.

Confidentiality

All Employees will be asked to sign the **Confidentiality Policy** either before employment, during employment, or on an ongoing basis. If at any time an Employee has a question about whether something should be considered confidential, the Employee should assume that the information is confidential until confirmation from the Department Manager has been obtained either way.

PROCEDURE

N/A

DOCUMENTS

Confidentiality Policy