



**VALUECLICK, INC. BUSINESS POLICIES &  
CODE OF ETHICS**  
*LAST UPDATED: October 2009*



*Tom Vadnais  
Chief Executive Officer*

To All ValueClick Employees:

ValueClick, Inc. and its subsidiaries (together, “ValueClick” or the “Company”) have a fundamental commitment to business ethics and to complying with the laws that regulate our business. We are committed to an environment that fosters honesty and integrity. To that end, we have developed this Business Policies & Code of Ethics (the “Code”). In addition, we have established a compliance program (the “Compliance Program”) designed to ensure that we have in place policies and procedures that are reasonably designed to prevent and detect violations of the Code or any applicable law, policy or regulation.

The Code applies to all employees, directors, and officers of ValueClick. As part of our Compliance Program, we have formed a Disclosure Committee and designated an outside compliance attorney whose names and telephone numbers are available and published on the Company intranet. In addition, the Chairman of the Audit Committee of the Board of Directors serves as a compliance contact for any violation related to ValueClick’s financial practices and dealings.

These resources are available to report apparent violations and may be used to address questions concerning the Code and Compliance Program. We encourage all employees to ask questions regarding the application of the Code. Employees may direct such questions to their manager (in the absence of an actual or potential conflict of interest), the Vice President of Human Resources, a member of the Disclosure Committee, the outside compliance attorney or the Chairman of the Audit Committee. Directors should raise any questions with a member of the Disclosure Committee, the outside compliance attorney or the Chairman of the Audit Committee.

While each individual employee is ultimately responsible for his or her compliance with the Code, every manager will also be responsible for administering the Code as it applies to employees and operations within that manager’s area of supervision. Managers should coordinate these tasks with appropriate compliance personnel. Managers may not delegate this responsibility.

If an employee observes or becomes aware of a situation that the employee perceives to be a violation of the Code, the employee has an obligation to notify his or her manager, a member of the Disclosure Committee as defined herein on page thirteen (13), the Vice President of Human Resources or the Chairman of the Audit Committee (together, “Compliance Officers”) unless the Code directs otherwise. Violations involving a manager should be reported directly to the Vice President of Human Resources or a Compliance Officer, not to or through the manager. In any case, when a manager receives

a report of a violation, it will be the manager's responsibility to handle the matter in consultation with a Compliance Officer. Directors should report any alleged violation with a member of the Disclosure Committee, the outside compliance attorney or the Chairman of the Audit Committee.

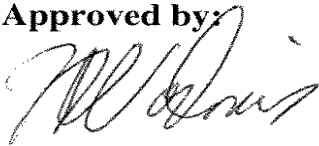
Employees who in good faith report a perceived violation to a Compliance Officer shall be treated fairly and respectfully. If an employee reporting a violation wishes to maintain anonymity, all reasonable steps will be taken to keep the employee's identity confidential. The communications will be taken seriously and, if warranted, any reports of violations will be investigated.

In order to make sure that all employees understand their responsibilities under the Code, the Compliance Program includes training requirements. New employees will receive an introductory briefing on the elements of the Code as part of their orientation.

The Code is available in printed form and also on the Company's intranet. Every employee must read and understand the Code. All employees are required, as a condition of employment, to provide the Company with a certification (attached hereto) that they have read and understand the Code. Employees will also be required to sign an annual verification that they have no reasonable basis to suspect that the Company or any person acting on behalf of the Company has engaged in any conduct in violation of the Code.

If any provision of the Code is held by any court of competent jurisdiction to be illegal, null or void or against public policy, the remaining provisions of the Code shall remain in full force and effect. ValueClick shall in good faith attempt to modify any invalidated provision to carry out its stated intentions after such determination has been made by a court of competent jurisdiction.

ValueClick is committed to creating a work environment where employees feel that, if they are doing something reasonable and in good faith, they will not be unfairly subjected to disciplinary action. As such, the Company encourages employees to disclose (either at the outset of their employment or as soon the need arises), any current or potential conflicts with this Code that exist or might reasonably be expected to arise during the course of their employment. The Company is vested with discretion to determine whether violations of the Code should be excused because they were either inadvertent and/or resulting from a good faith effort by the employee to comply with the Code. Candid disclosure in advance of such potential conflicts is a significant factor in the exercise of this discretion.

**Approved by:**  
  
Chief Executive Officer

September 2009

## TABLE OF CONTENTS

	<b>PAGE</b>
GLOSSARY OF TERMS	5
<b>I. SCOPE AND RAMIFICATIONS</b>	6
<b>II. CONFIDENTIALITY</b>	7
<b>III. CONFLICTS OF INTEREST AND RELATED PARTY TRANSACTIONS</b>	9
<b>IV. DRUGS &amp; ALCOHOL</b>	10
<b>V. ENTERTAINMENT, RECEIVING &amp; PROVIDING GIFTS</b>	10
<b>VI. POLICY AGAINST DISCRIMINATION &amp; HARASSMENT</b>	11
<b>VII. POLICY AGAINST HUMAN TRAFFICKING</b>	12
<b>VIII. ANTI-FRAUD POLICY</b>	12
<b>IX. COMPLAINT PROCEDURE FOR SUSPECTED FRAUDULENT ACTIVITY</b>	16
<b>X. ELECTRONIC COMMUNICATION</b>	17
<b>XII. SOCIAL NETWORKING GUIDELINES</b>	20
<b>XII. COPYRIGHTS</b>	22
<b>XIII. DOCUMENT RETENTION POLICY</b>	22
<b>XIV. RECORDS &amp; ACCOUNTING INTEGRITY</b>	24
<b>EMPLOYEE ACKNOWLEDGEMENT AND ACCEPTANCE</b>	25
<b>ANNEX A – COMPLIANCE OFFICERS</b>	26
<b>ANNEX B – POSSIBLE INDICATORS OF FRAUD</b>	27
<b>ANNEX C – HYPOTHETICAL EXAMPLES OF FRAUD</b>	29

## **GLOSSARY OF TERMS**

**COMPANY PARTIES** - Company's customers, vendors or employees.

**COMPLIANCE OFFICERS** – (i) the Vice President of Human Resources, (ii) the General Counsel or other in-house counsel; (iii) any member of the Disclosure Committee; (iv) the outside compliance attorney or (v) the Chairman of the Audit Committee. The names and contact information for each of these individuals is included in Annex A and is also available on the Company's intranet site, VC Central (<http://myvalueclick.com>).

**CONFIDENTIAL INFORMATION** - includes information in whatever form regarding the business, accounts, finances, trading, planning, software or know-how of the Company and existing or prospective customers or clients.

**FRAUD** - inducing a course of action by deceit or other dishonest conduct, involving acts of omissions or the making of false statements, orally or in writing, with the objective of obtaining money or other benefits from or of evading a liability to, the Company. Fraud is not restricted to deceit for the purpose of obtaining monetary or material benefits but also may include intangible benefits such as status and information.

**OFFENSE** - means an act or omission in violation of this Code.

**SEC** – Securities and Exchange Commission

**SERIOUS IMPROPER CONDUCT** - where an employee has engaged in conduct (other than criminal conduct) that: (i) adversely affects, or could adversely affect, directly or indirectly, the honest or impartial performance of the functions of another employee; (ii) constitutes or involves the performance of the employee's functions in a manner that is not honest or is not impartial; (iii) constitutes or involves a breach of the trust placed in the employee by reason of his or her employment; or (iv) involves the misuse of information or material that the employee has acquired in connection with his or her functions as an employee.

Serious improper conduct could, for example, include: breach of public trust; neglect of duty, abuse of authority; telling lies; favoritism; and bias. No list is exhaustive but Annex C – Hypothetical Examples of Fraud is attached for illustrative purposes.

## I. SCOPE AND RAMIFICATIONS

ValueClick's objective is to maintain a productive, positive and honest work environment. In order to provide such an environment and to comply with applicable law, we have adopted this Code, which establishes rules and standards regarding employee behavior and performance and constitutes a part of the terms and conditions of employment of each employee of the Company. Conduct which either (i) violates the rules and standards embodied in the Code, (ii) interferes with the Company's operations, (iii) brings discredit to the Company or (iv) is offensive to the Company's customers, vendors or Company employees ("**Company Parties**"), will not be tolerated and will subject offending employees to disciplinary action.

---

Listed below are examples of prohibited conduct which will subject the employee involved to disciplinary action including, but not limited to, termination:

- **breach** of the Code;
- direct **refusal** to respect and follow management's instructions concerning a job-related matter (i.e., insubordination);
- **violation** of state and/or federal law;
- employee **harassment** of any kind, whether it be relating to race, religious creed, color, age, sex, sexual orientation, national origin, ancestry, religion, marital status, medical condition as defined under applicable law, disability (sensory, mental or physical), HIV or AIDS status, military service, arrest and conviction records, or any other category protected by applicable law;
- the unauthorized **use of alcoholic beverages** while on Company premises and on Company time, or reporting for work while under the influence of alcohol;
- the unlawful possession, manufacture, sale, distribution or **use of a controlled substance**, or reporting for work while under the influence of such a substance, other than medically prescribed drugs;
- **theft**, misuse or willful destruction of property belonging to Company or Company Parties or the failure to report any knowledge of such theft;
- **falsifying** any Company record or report, books of account, records, reports and financial statements, including Travel and Expense Reports and time sheets; or
- any conduct placing ValueClick in **disrepute** because of its association with you.

In addition, inadequate or poor work performance may also be grounds for disciplinary action or termination. The Company has the right to terminate an employee's employment *with or without cause* (except where prohibited by applicable law or a written employment contract). Depending

upon the circumstances surrounding a given situation, the Company maintains the right to carry out whatever disciplinary action is deemed appropriate and to report any suspected criminal activity to the proper authorities where the Company deems it advisable or required.

The Company prohibits and will not condone any form of retaliation against individuals who in good faith report unwelcome conduct or who cooperate in the investigation of such reports. In accordance with this policy, the Company will take appropriate disciplinary action for any such retaliation, up to and including termination.

If any provision of the Code is held by any court of competent jurisdiction to be illegal, null or void or against public policy, the remaining provisions of the Code shall remain in full force and effect. The Company shall in good faith attempt to modify any invalidated provision to carry out its stated intentions after such determination has been made by a court of competent jurisdiction.

## II. CONFIDENTIALITY



As an employee, you may have access to proprietary and confidential information concerning the Company's business and employees, and the business of the Company's clients and suppliers. Proprietary and confidential information may include any documents or information concerning the Company's business that is not generally known to the public that could be valuable to the Company's competitors which the Company takes reasonable measures to protect. You are required to keep such information confidential during your employment as well as thereafter, and not to use, disclose or communicate that confidential information other than in your role as an employee and subject to a confidentiality agreement approved by the Legal Department.

---

As a general matter, any access you will have to proprietary and confidential information is on a need-to-know basis. Unnecessary or unauthorized efforts to secure confidential information could constitute grounds for disciplinary action against you, including termination of employment. For instance, it is a violation to comb the Company's computers or files without appropriate consent.

Serious problems could be caused by the unauthorized disclosure of information pertaining to internal matters or developments, or by the unauthorized disclosure of any non-public, privileged or proprietary information. In addition to possibly violating the law, such disclosure could, among other things, competitively disadvantage the Company or breach the confidence of a customer of the Company.

### CONFIDENTIAL INFORMATION

The use of the term "**Confidential Information**" includes information in whatever form regarding the business, accounts, finances, trading, planning, software or know-how of the Company and

*ValueClick Business Policies & Code of Ethics*

Page 7 of 29

Last Revised 10/1/09

existing or prospective customers, clients, and employees. Company records, reports, data, software and documents are confidential and employees are not permitted to remove, make copies, disclose or release them (in whole or in part) to persons who are not directors, officers or employees of the Company without prior approval of their manager.

Except as required in the performance of an employee's duties, or if required by law after consulting with the Company's General Counsel, employees should not discuss Company business with anyone who does not work for ValueClick and never discuss confidential business transactions with anyone, including another Company employee, who does not have a direct association with the transaction. Furthermore, employees must refrain from discussing or disclosing Confidential Information while in any non-private setting.

If employees are questioned by someone outside their department and they are concerned about the appropriateness of giving that person information, they are not required to answer. Instead, as politely as possible, they should refer the inquiry to their manager and reference the Code. Any inappropriate inquiries from someone outside the Company concerning the Company's business should be referred to the Company's General Counsel and/or Vice President of Corporate Communications.

#### **DUTIES AFTER LEAVING THE COMPANY**

Moreover, employees owe a continuing obligation of confidentiality after leaving the Company's employment, including compliance with the Company's Confidential Information and Invention Assignment Agreement. Employees may not disclose the Company's Confidential Information to any third-party after leaving employment except with the prior written consent of the Company or as required by applicable law.

Upon termination of employment, employees will be required to sign a declaration, in form and substance satisfactory to the Company, confirming their continued obligation of confidentiality owed to the Company and confirming they have returned all company property and any and all company documents. Company documents are the sole property of ValueClick.

#### **PRIVILEGED AND THIRD PARTY INFORMATION**

In addition to protecting our own proprietary information, it is the policy of the Company to respect the proprietary information of others. Should any employee be furnished with such information or become aware of information that he or she believes may have been misappropriated from another party, that employee should immediately report the event to a Compliance Officer.

No current or former employee shall disclose any attorney-client privileged information or any attorney work product without the prior written consent of the General Counsel of the Company.

### III. CONFLICTS OF INTEREST AND RELATED PARTY TRANSACTIONS



ValueClick strives to conduct its affairs in strict compliance with the letter and spirit of the law and to adhere to the highest principles of business ethics. Accordingly, all directors, officers, employees, and independent contractors, including members of their immediate household, must avoid activities and relationships which are in conflict, or give the appearance of being in conflict, with these principles and with the interests of the Company.

---

A conflict of interest may arise when an individual receives improper personal benefits as a result of his or her position with ValueClick, or when an individual has other duties, responsibilities or obligations that run counter to his or her duty to the Company. A conflict of interest or potential conflict of interest may be resolved or avoided if it is appropriately disclosed and approved in writing by a Compliance Officer, or, if the conflict involves an officer or director of the Company, it must be disclosed and approved in writing by the Audit Committee of the Board of Directors. In some instances, disclosure may not be sufficient and the Company may require that the conduct be stopped or that actions taken be reversed where possible. Any actual or potential conflict of interest must be reported to a Compliance Officer.

This Code does not attempt to describe all possible conflicts of interest that could develop. Some of the more common conflicts that must be avoided are described below.

- Accepting or offering gifts, entertainment or favors may be improper or embarrassing to the Company if they have a value beyond what is normal and customary in the Company's business or they are being offered in order to influence an individual's actions.
- Initiating or approving personnel actions affecting reward or punishment of employees or applicants where there is a family relationship or is or appears to be a personal or social involvement.
- Investing or holding outside directorships in suppliers, customers or competing companies, including financial speculation, where such investment or directorship might influence in any manner a decision or course of action taken in the scope of performing duties for the Company.
- Borrowing from or lending to customers or suppliers.

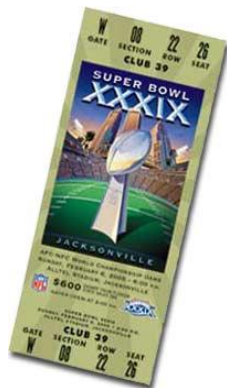
- Acquiring or having an interest in real estate that the Company owns or proposes to acquire.
- Using Company assets, labor, or information other than for the Company's benefit or the legitimate business purposes of the Company.
- Consulting, owning, operating or having an affiliation or controlling interest in an advertiser, publisher, affiliate or performance marketing business that is revenue generating.

#### IV. DRUGS & ALCOHOL



The Company prohibits the unauthorized use of alcoholic beverages while on Company premises, on Company time, or reporting for work while under the influence of alcohol. Likewise, the Company prohibits the unlawful possession, manufacture, sale, distribution or use of a controlled substance, or reporting for work while under the influence of such a substance, other than medically prescribed drugs. This policy also requires that the Company abide by applicable laws and regulations relative to the use of alcohol or other controlled substances.

#### V. ENTERTAINMENT, RECEIVING AND PROVIDING GIFTS



The Company does not permit the giving or receiving of cash or cash equivalent gifts (e.g., cash, checks, gift cards or gift certificates, etc) to our employees. Examples of when this policy may be relevant are at holidays when a manager or executive considers giving out gift certificates or cash awards, or at other times during the year when one time cash or cash equivalent distributions are considered as “perks”. In the rare event that an executive feels that these types of awards are a necessity, they may only be given with the prior approval of the business unit or department head and the Chief Financial Officer or Vice President of Human Resources. Such approval will be documented on the Company's regular PCN form. In this instance, the amounts will be considered taxable income to the employee(s), regardless of the form of the award and will be included in the employee's income for their W-2.

In addition the Company does not permit the giving or receiving of cash or cash equivalent gifts (e.g., cash, checks, gift cards or gift certificates, etc.) or trips from or to our vendors, publishers, advertisers, etc. In the rare event that an executive feels that these types of awards are a necessity, they may only be given with the prior approval of the business unit or department head and the Chief Financial Officer or Vice President of Human Resources. If any such items are received in the future, they are to be immediately declined or returned to the sender. (See VC Central for a draft of a letter to be used to return such items.)

## **VI. POLICY AGAINST DISCRIMINATION & HARASSMENT**



The Company prohibits discrimination against any employee or prospective employee on the basis of sex, race, color, age, religion, sexual preference, marital status, national origin, disability, ancestry, political opinion or any other basis prohibited by the laws that govern our operations.

The Company also prohibits all forms of unlawful harassment. The Company expects all personnel to adhere to a simple standard, namely, that all employees must be treated with respect. The Company will vigorously enforce its policy regarding harassment. All employees are expected to understand what constitutes harassment and accordingly avoid behavior or situations which could have even the appearance of or be interpreted as harassment of another person.

---

Harassment is not an occasional compliment or other generally acceptable social behavior. It refers to any conduct, comment, gesture or contact (e.g., relating to race, religious creed, color, age, sex, sexual orientation, national origin, ancestry, religion, marital status, medical condition as defined under applicable law, disability (sensory, mental or physical), HIV or AIDS status, military service, arrest and conviction records, or any other category protected by applicable law) that is likely to cause offense or humiliation to a reasonable person or that might, on reasonable grounds, be perceived by a reasonable person as placing a condition on their employment or on any opportunity for training or promotion.

### **REPORTING AND COMPLAINT PROCEDURES**

If an employee feels that he or she has been the victim of any form of harassment, he or she should promptly contact (i) his or her manager who may report it to another Compliance Officer or (ii) a Compliance Officer in cases involving the manager. If the employee fails to report the occurrence of an alleged harassment within a reasonable time, the Company's ability to conduct a thorough investigation and respond effectively to the situation may be limited. For this reason, employees are encouraged, if they feel that they have been the target of harassment, to report the incident promptly. Any harassment reported to a manager must be reported by that manager to the General Counsel and/or the Vice President of Human Resources.

This initial report of harassment can be oral or written, but an employee will be asked to submit a written and signed statement of the complaint within one week of the initial report. Upon receipt of the written statement, the Company will conduct a fact-finding investigation.

Reports will be investigated with due regard for the privacy of those involved. Any employee found to have harassed a fellow employee or subordinate will be subject to disciplinary action, including possible termination. The Company will also take any additional action necessary to appropriately remedy the situation. No adverse employment action will be taken against any employee making a good faith report of alleged harassment.

Harassment is outside the course and scope of every employee's job-related duties and the individual who makes unwelcome advances, threatens or in any way harasses another employee is personally liable for such actions and their consequences.

## **VII. POLICY AGAINST HUMAN TRAFFICKING**

Human trafficking is the modern day practice of slavery. Also known as "trafficking in persons", it refers to the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs.

The United States Government has adopted a zero tolerance policy regarding trafficking in persons and The Company thoroughly prohibits any involvement in such behavior.

## **VIII. ANTI-FRAUD POLICY**



To avoid fraudulent behavior by implementing preventative and detective strategies and establishing controls relating to fraudulent activities, and to outline investigative and reporting processes in connection with such activities. The aim of this policy is to stimulate an environment that actively discourages fraudulent behavior but in the event that such occurs, to provide a transparent framework for addressing such occurrences.

[Annex B](#) – Possible Indicators of Fraud is included for guidance. The Company has an obligation to follow up on such reports and take the appropriate steps to discourage such behavior. This policy is not a mechanism for the resolution of personal disputes or grievance issues that cannot be resolved by other procedure.

## **ROLES AND RESPONSIBILITIES**

### DISCLOSURE COMMITTEE

The Disclosure Committee has the ultimate responsibility for the prevention and detection of fraud and is responsible for ensuring that appropriate and effective internal control systems and accounting are in place. The Disclosure Committee is responsible for the receipt of complaints in accordance with this policy and for the coordination, and conduct where appropriate, of preliminary investigations within the Company. The Disclosure Committee also oversees any formal investigations into any reported allegations of fraudulent behavior. The Disclosure Committee has the responsibility of referring to, or notifying, the Chief Executive Officer and the Audit Committee of any allegations of fraudulent behavior within the Company.

The Disclosure Committee is convened both on an as-needed basis to oversee preliminary investigations and quarterly to review any allegations or investigations involving fraud and to confirm that neither the Committee nor any other Compliance Officers are aware of other instances of fraud. This group consists of the following personnel:

- Chief Financial Officer;
- General Counsel; and
- Vice President of Human Resources

The names and contact information for each of these individuals is included in [Annex A](#) and is also available on the Company's intranet site, VC Central ([www.my.valueclick.com](http://www.my.valueclick.com)).

### SENIOR EXECUTIVES AND GENERAL MANAGERS

All levels of management are responsible for the prevention and detection of fraud and for the implementation and operation of controls that minimize fraudulent activity within their areas of responsibility. It is the responsibility of all managers, within their day-to-day operations, to ensure that there are mechanisms in place within their areas of responsibility to assist with:

- Assessment of the risk of fraudulent behavior through awareness of the risks; and exposures inherent in their areas of responsibility;
- Promotion of awareness of ethical principles subscribed to by the Company;
- Education of employees about fraud prevention and detection;
- Promotion of a positive and appropriate attitude towards compliance with laws, rules and regulations; and
- Prompt and positive responses to all allegations or indications of fraudulent or wrongful acts.

Where managers do not have the expertise to evaluate internal controls in their areas of responsibility, they should call on support from the Disclosure Committee.

Managers should be aware of common indicators and symptoms of fraudulent or other wrongful acts and respond to those indicators as appropriate. Details of common areas of fraud and indicators of fraud are described in [Annex B](#).

#### COMPANY PERSONNEL

This policy is applicable to all employees and is taken to include contract personnel engaged by the Company. Employees are responsible for compliance with controls, policies and procedures. Employees should be aware of the signs of fraudulent activity and, to that end we have provided examples of such activity in [Annexes B](#) and [C](#).

If employees become aware of fraudulent activity, there is a duty to immediately report such activity to a member of the Disclosure Committee. Employees are expected to assist with any inquiries and investigations pertaining to fraudulent activity.

#### **COMPLAINANT PROTECTION AT VALUECLICK**

The Company will treat all complaints confidentially and with the utmost professionalism. The Company does not, and will not, condone any retaliation of any kind against an employee who comes forward with a good faith ethical concern or complaint.

ValueClick has a duty to protect persons making complaints to it in regard to fraudulent behavior and is required to (i) investigate disclosures and remedy any actual defects or wrongdoings; and (ii) provide protection for any good faith complainant including, confidentiality, employment protection (i.e., protection from retaliation) and, where appropriate, immunity from any civil liability.

#### **COMPLAINT GUIDELINES**

Complaints can be written or verbal. If verbal complaints are made, then the person receiving the complaint shall create a written record of the complaint. It is preferred that complaints about suspected fraudulent behavior be written, dated and signed by the complainant. The complaint should identify or provide evidence of the following to the extent that this detail is known or available to the complainant:

- The location of the alleged incident(s).
- Key personnel involved in the alleged incident(s).
- The nature of the alleged incident(s).
- The time period over which the alleged incident(s) occurred.
- An estimate of the monetary value, if appropriate, associated with the alleged incident(s).
- Documentary evidence in support of the alleged incident(s).

Complaints should be made to a member of the Disclosure Committee following the escalation procedure set forth in Section VIII.

Employees are encouraged not to make anonymous complaints as they may be difficult to pursue if further information is required and anonymity will prevent the Company from reporting back to any complainant. Well-substantiated anonymous complaints will, however, receive due and proper consideration.

#### **CONFIDENTIALITY**

- Managers are required to maintain confidentiality with respect to complaints or matters referred to them;
- There is a need to maintain confidentiality, and the employee subject to the complaint should not be initially advised of any inquiries as this may prejudice future investigations. Information pursuant to any preliminary inquiry or investigation shall only be made available on a need-to-know basis. Whether notice shall be provided to the employee who is the subject of the complaint shall be based on the advice of the Disclosure Committee;
- Any records arising from initial inquiries and preliminary investigations should be placed in a confidential central legal records file created for the complaint;
- Great care needs to be taken in the investigation of suspected fraudulent behavior to avoid:
  - unfounded and incorrect accusations,
  - unnecessarily and prematurely alerting individuals against whom allegations have been made, and
  - making statements that could expose the Company to legal liability for damages arising from a wrongful accusation.
- Whistleblowers or any other Company employees should not:
  - attempt to personally conduct any formal investigations or interviews in order to determine whether or not a suspected activity is improper. However, this does not preclude management from conducting appropriate preliminary inquiries to determine whether or not there is a basis for the complaint and further action. Such preliminary inquiries must consider the constraints imposed by this policy.
  - contact the suspected individual(s) to determine facts or demand restitution.
  - discuss any facts, suspicions or allegations associated with the complaint with anyone, unless specifically directed by a Disclosure Committee

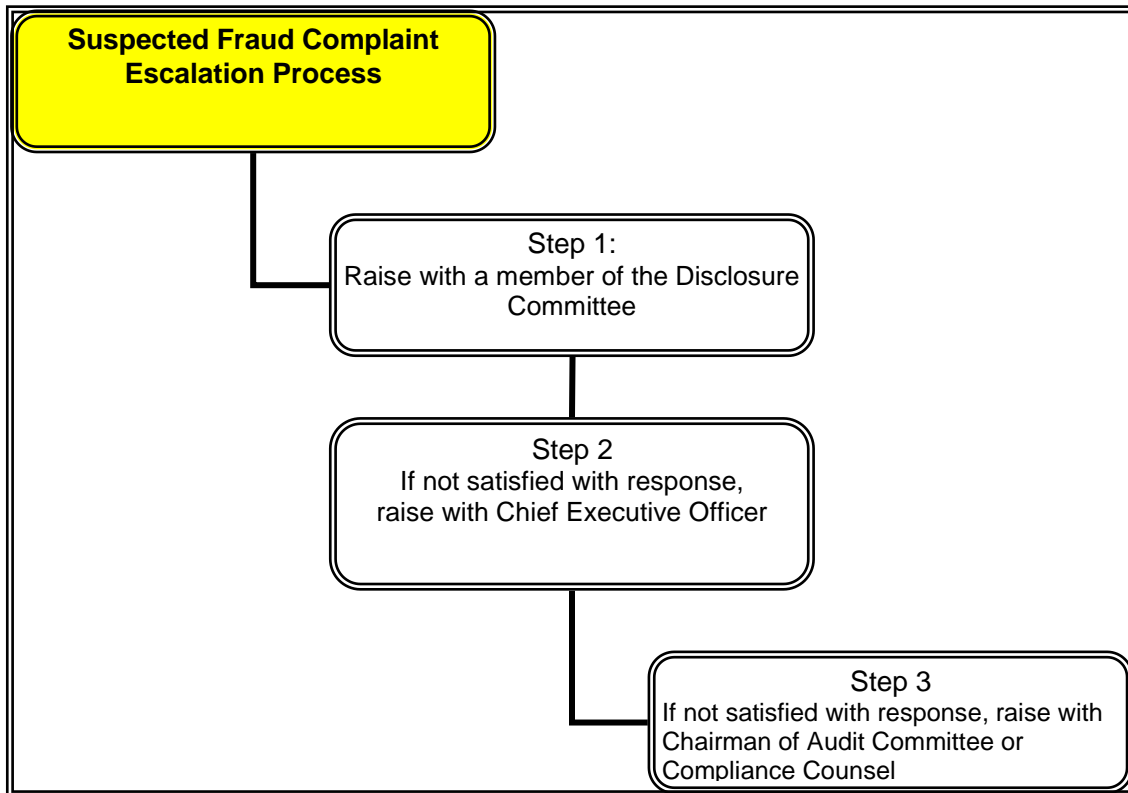
member or officers from law enforcement or regulatory agencies.

**REPORTING**

Reports on investigations prepared under this policy will, at a minimum, be sent to the Disclosure Committee and the Audit Committee as soon as is practicable. Reports may also be sent to appropriate authorities, but only with the express consent of the Chief Executive Officer, Chief Financial Officer or General Counsel, who shall also notify the Chief Executive Officer, Chief Financial Officer, the General Counsel and the Chairperson of the Audit Committee.

**IX. COMPLAINT  
PROCEDURE FOR  
SUSPECTED  
FRAUDULENT  
ACTIVITY**

The complaint procedure is for employees who may have concerns regarding perceived fraud. If an employee feels that he or she has a concern or complaint concerning fraud, the procedure for expressing such concern or complaint is as follows:



The names and contact information for each of these individuals is included in [Annex A](#) and is also available on the Company's intranet site, VC Central (<http://.my.valueclick.com>).

The Company will treat all complaints confidentially and with the utmost professionalism. If an employee desires, he or she may submit any concerns or complaints on an anonymous basis, and his or her concerns or complaints will be addressed in the same manner as any other complaints. The Company does not, and will not, condone any retaliation of any kind against an employee who comes forward with a good faith ethical concern or complaint.

## X. ELECTRONIC COMMUNICATION



The Company provides electronic communication tools to help improve productivity and enable you to provide efficient, high-quality work. Electronic communications include all aspects of voice, video, and data communications, such as voice mail, e-mail, fax, and Internet access. The Company views electronic communications as a business tool provided to employees at significant cost. We encourage you to use these electronic communications subject to the requirements set forth below.

---

You are required to use your access to these tools for business-related purposes, e.g., to communicate with customers and suppliers, to research relevant topics and obtain useful business information. However, personal use of the Company's e-mail system is permitted, so long as such use is reasonable and does not otherwise interfere with legitimate business uses. While using electronic communication, you must conduct yourself honestly and appropriately, and respect the intellectual property rights, privacy and prerogatives of others.

All Company policies apply to your conduct on electronic communications, especially (but not exclusively) those that deal with intellectual property protection, discrimination, misuse of Company resources, sexual harassment, data security and confidentiality. **In addition, please note that email solicitations (whether in bulk or sent by a single sales persons) must comply with the requirements of the CAN-SPAM Act of 2003.**

The Company has software and systems in place that can monitor and record all electronic communications usage. The Company wants employees to be aware that our security systems are capable of recording (for each and every user) each website visit, each chat, newsgroup or e-mail message and each file transfer into and out of our internal network. The Company reserves the right to monitor these communications at any time, without

notice to the employees. No employee should have any expectation of privacy as to his or her usage of electronic communication tools. The Company reserves the right to inspect any and all files of any form of communication stored in private areas of our network in order to assure compliance with policy.

The Company prohibits the display of any kind of sexually explicit image or document on any Company system other than as required for business purposes. In addition, sexually explicit material may not be accessed, archived, stored, distributed, edited or recorded using our network or computing resources other than as may be required for legitimate business purposes. If an employee finds that he or she is connected to a site that contains sexually explicit or offensive material, he or she should disconnect from that site immediately.

No employee may use the Company's electronic communication to overload any computer system or network or to circumvent any system intended to protect the privacy or security of another user. Abuse of access privileges or passwords by unauthorized entry into another employee's system or files, or into the Company's internal or external networks, or the distribution of messages or materials that are not consistent with the policies for appropriate workplace conduct, are subject to appropriate disciplinary action up to and including dismissal. In some cases, the abuse of access privileges may be illegal, and the violator may be subject to legal penalties.

Use of Company electronic communication tools to commit infractions such as misuse of Company assets or resources, discrimination, sexual harassment, unauthorized public statements and misappropriation or theft of intellectual property are also prohibited.

User IDs and passwords help maintain individual accountability for electronic communication usage. Any employee who obtains a password and User ID must keep these confidential. These passwords should not be shared with other parties and should be changed frequently. Employees should set passwords that are not easy to decode and in particular should avoid use of familiar terms such as their family member names, birthdates and other data sets that can be easily associated with them. Employees should also not post passwords in visible and accessible places. In particular, employees with laptops provided for travel access should make sure that the passwords are not in the laptop files as well. Laptops can be stolen or accessed by unauthorized parties and remote access can be obtained if passwords are easily located. Employees should immediately call the IT Help Desk to lock out system access and change passwords if laptops are stolen or lost.

Employees learning of any technical misuse of the Company's electronic communications systems should notify their Department Manager. Employees experiencing system-related technical or functional problems should notify the IT Department. Employees aware of other system misuse (e.g., messages dealing with sexual harassment, racial slurs, etc.), are encouraged to notify a Compliance Officer or their designated Human Resources representative.

To the extent required by Company policies or prudent business practices, voice, data, files and images (hereinafter referred to as "electronic records") should be saved to the appropriate drives if they relate to the Company's business. All e-mail kept in the e-mail section may be deleted at the end of every calendar quarter or sooner if file storage limitations are encountered. The Company's general policy is that employees should delete all e-mail which is greater than 30 days old, unless such policy is tolled or suspended by litigation or other legitimate business reasons. Employees will be notified by the General Counsel if the 30-day policy has been suspended.

Employees should exercise discretion in the dissemination of electronic records. These records should be sent only to persons who need the information for business purposes. Employees should refrain from mass cc's of electronic records to ensure that we do not inundate other employees with information they do not need.

The Company policies concerning confidentiality of information also apply to information transmitted by e-mail. Use of e-mail raises additional concerns related to confidentiality. The Company has implemented various security measures designed to protect the confidentiality of corporate information transmitted through the internal e-mail system. E-mail systems operated by third-parties should not be considered secure and therefore should not be used to transmit confidential information unless you obtain reasonable assurances as to confidentiality.

Company personnel should not participate in any electronic forum discussing and/or disclosing information about the Company, its customers, suppliers or other persons with which the Company does business or involving any Company confidential information. In no case is any employee of the Company authorized to make any defamatory statement using the Company's electronic communications system. Violation of this provision shall result in appropriate disciplinary action including, but not limited to, dismissal.

Even in the case of the Company's internal e-mail system, each employee is responsible for using e-mail in a manner that preserves the confidentiality of information transmitted through the system. For example, each employee is responsible for maintaining the confidentiality of his or her passwords and identification numbers and any attorney-client communications. In addition, each employee has the responsibility not to send or forward e-mail to any person who does not need to know the information in the e-mail for business purposes. Likewise, e-mails should not be reviewed by employees who are not an addressed recipient of the e-mail, unless authorized by the sender of the e-mail, an addressed recipient of the e-mail or a member of senior management exercising the Company's rights to monitor electronic communications.

Back-up tapes are made of the entire network and record information transmitted by e-mail (including e-mail that an employee may have intended to delete from the system). As a result, material transmitted through e-mail may be subject to disclosure to unintended third-parties (for example, in a litigation context), even if a "hard copy" of the e-mail is not made. Accordingly, each e-mail should contain only the specific facts and other information that need to be communicated for business reasons. Before saving or sending

an e-mail, users should consider whether any information contained in the communication might be misconstrued if reviewed by a third-party.

The Company has installed firewalls to assure the safety and security of the Company's network. Any employee who attempts to disable, defeat or circumvent any Company security facility may be subject to dismissal.

## **XI. SOCIAL NETWORKING GUIDELINES**

### **Authorized Poster and Employee Guidelines:**

- General for all employees—there should be no Company posts and similar social networking communications unless they are done by individuals who are specifically authorized in writing by the employee's divisional General Manager, and the posts are in accordance with the below. Company posts include posts about Company initiatives, positions, industry initiatives, matters related to the Company, and the like. Notwithstanding the foregoing, all employees may repost Company-authorized posts posted by authorized Company posters, provided the employees *only* link to the Company posts *without* any additional commentary, summaries, etc. If you are using these forums for sales prospecting and /or one-on-one client interaction as it relates to your job area and responsibility, feel free to do so using a professional manner and under the terms of use associated with each forum.
- Only employees who are authorized to make Company posts may list their Company Twitter and/or other social networking accounts/logins in Company signature blocks or other Company materials.
- If employees are connected to clients and other industry-related individuals on social networking platforms, the communications with these individuals on the platforms should be restricted to general communications compliant with these guidelines and that stay away from communications similar to Company posts (described above).
- All employees should follow the Terms of Use and any other applicable regulations of the service(s)/platform(s) used.
- Blogging, tweeting or posting may only be done on Company time if it is specifically a part of an employee's assigned duties and responsibilities and permitted by these guidelines.
  - There is no expectation of privacy when using Company equipment.
  - If you are authorized to post, do not let posting conflict with your other job duties and responsibilities.
- Remember these are *public* forums.
- Whenever you are posting, keep a professional manner.
- You are personally responsible for your content. Managers and executives may be held to an even higher level of responsibility.
- When quoting someone, use quotes and give proper attribution.

- Do not comment on rumors or any miscellaneous postings, even if such postings are inaccurate.
- Follow all Company policies, including those in the Employee Handbook and Code of Conduct.
- Report inappropriate social networking behavior of employees to your HR Business Partner who will discuss such behavior with the VP of HR.
- Reflect and review carefully before posting.
- There should be absolutely no remarks that are offensive in any way.
- Respect proprietary and confidential information of the Company and others.
- Authorized posts may not cite specific clients unless written permission is obtained from the cited clients specifically approving such post(s).
- Use respect.
- All statements should be true and not be misleading.
- Do not post or summarize in any way any internal Company/business communications.
- Follow all applicable laws and regulations including, but not limited to copyright, Trademark, privacy, defamation, harassment, and financial disclosure laws.
- Do not address Company financial matters or make performance predictions, including, but not limited to commission rates, billing terms, account sales, revenue, profit, margin, projected sales, etc. Make no references to high, low or average rates.
- Unless specifically authorized to do so in writing by the relevant division's General Manager, do not use Company logos and Trademarks on the relevant platform, including, but not limited to, in posts and logins/account names.
- Do not disparage competitors and others.
- If a member of the news media contacts you regarding the Company or its business in any form, direct all inquiries to Gary Fuges.
- Do not comment on any Company or Company-related legal matters.
- There should be no discussion of customer wins or losses unless it has already been disclosed in a public press release. If it has already been disclosed in a public press release only cite/link to the release. Do not add comments or summaries about the release.

**Authorized Poster Guidelines [follow the above and below guidelines]:**

- Check the relevant platform(s)'s terms of use and related policies often to see if they have been updated, and be certain to comply with all such terms and policies.
- Re-posting relevant and appropriate third party posts/links without additional commentary is permitted if this practice is standard and allowable by the networking forum and the third party and proper attribution is given.
- Use spell check and grammar check.

- Any postings should be reviewed by a second person (to be designated by the division's General Manager) for compliance with these guidelines, quality control of content, format, grammar, spelling, etc.

\*\* Not everything is covered in these guidelines. All employees will sign an acknowledgement of these policies/guidelines during the annual policy acknowledgement process. Violation of the guidelines may result in disciplinary action up to and including termination.

## XII. COPYRIGHTS



Images and contents of websites on the Internet may be subject to copyright laws. While you may make printouts of the contents of a third-party website, the particular website may prohibit re-use of the images or the contents. As a matter of precaution, these images and contents should not be incorporated in presentations or material prepared for Company use without the permission of the third-party website owner and/or our Legal Department.

All software that is the property of the Company can only be installed for use in hardware owned by the Company or hardware approved by the Company. This ensures that the Company does not violate copyright laws for software purchased.

---

## XIII. DOCUMENT RETENTION POLICY



ValueClick's general rule is as follows:

*All business records should be retained for not more than one (1) year after the calendar year in which they are prepared or acquired.*

There are a few exceptions to this rule for documents falling into the categories outlined below.

---

### THIRTY DAYS

- E-mail messages that remain in a user's inbox, deleted items, or sent mail folders are presumed to have no business value and should be automatically deleted after thirty (30) days.

## **FOUR YEARS**

- Records containing personal information of employees should be retained for four (4) years from the time the record is created unless otherwise directed by the Human Resources department and/or General Counsel.
- Sales contracts, purchase orders, leases, releases, agreements, and other contracts should be retained for a period of (4) four years after the calendar year in which the performance of the contract or other obligation was completed.

## **OTHER**

- All records that the Company is required to retain by law or contract, or which are the subject of special written arrangements, should be retained for the specified periods.
- Documents that the Office of the General Counsel determines to be relevant to current or pending judicial or agency proceedings or investigations must not be destroyed until after the final resolution of those proceedings.
- Drafts of documents should be discarded immediately upon completion of the final documents or final termination of discussions;
- All technical data such as engineering records, source code listings, test and reports should be retained for such period of time as determined by the project's manager and, in connection with patent or other intellectual property-related records, the General Counsel.
- Accounting and financial documents are governed by policies created by the Internal Revenue Service, the Securities and Exchange Commission (“SEC”) and other regulatory authorities.

All personnel should review the records detailed above at least semi-annually. In the event any legal action or government investigation is or is likely to be initiated, the General Counsel will order all destruction activities to be suspended immediately.

#### **XIV. RECORDS & ACCOUNTING INTEGRITY**



Accuracy and reliability in the preparation of all business records is mandated by law and is of critical importance to the Company's decision-making process and to the proper discharge of ValueClick's financial, legal and reporting obligations.

The books and records provisions of the U.S. Foreign Corrupt Practices Act and the Sarbanes-Oxley Act of 2002 require the Company to maintain accurate books and records and to devise an adequate system of internal controls. Reports and documents that ValueClick files with or submits to the SEC, and other public communications that ValueClick makes, should reflect full, fair, accurate, timely, and understandable disclosure of information.

**EMPLOYEE ACKNOWLEDGEMENT AND ACCEPTANCE**

I understand that the ValueClick, Inc. Business Policies & Code of Ethics (the “Code”) forms a part of my terms of employment or directorship.

I understand that it is my responsibility to read, understand, and keep up to date with the contents of the Code, and to seek clarification or further information if needed. I understand and accept all of the terms and conditions of the Code.

I understand that breach or violation of the Code may result in disciplinary action including, but not limited to, termination of my employment.

I acknowledge that I received a copy of the Code for my review and reference.

I acknowledge that I have been afforded the opportunity to ask any questions I have concerning the content of the Code and related Compliance Program.

I hereby acknowledge that I am unaware of any violations of the Code.

If I am aware of any violations, I acknowledge that I have reported the violations to the Company pursuant to the reporting procedures as outlined in the Code.

Signature \_\_\_\_\_


Date \_\_\_\_\_

Name \_\_\_\_\_

(Please print)

Sign and deliver to your Human Resources representative for filing in individual personnel file.

## ANNEX A – COMPLIANCE OFFICERS

	Title	Name	Email	Phone
	Vice President Human Resources	Ken Bauer	kbauer@valueclick.com	818-575-4542
	Vice President and General Counsel	Scott Barlow	sbarlow@valueclick.com	818-575-4510
	Chief Financial Officer	John Pitstick	jpitstick@valueclick.com	818-575-4758
	Outside Compliance Counsel	Brad Weirick Gibson, Dunn & Crutcher	bweirick@gibsondunn.com	213-229-7635
	Audit Committee Chairman	James Peters	jpgeters@yahoo.com	805-558-1683

## **ANNEX B - POSSIBLE INDICATORS OF FRAUD**

1. The following list contains some of the possible indicators of fraud. They are presented to heighten employee awareness of potential control lapses that make an environment more conducive to fraudulent behavior. These indicators can be viewed in isolation or in combination, although the latter will generally indicate that circumstances of fraudulent or corrupt behavior are a distinct possibility.
2. Employees need to proceed with caution, as the presence of one or more of the following indicators of fraud or corruption does not mean that such behavior is occurring. Such lapses in control may be the result of other factors. As a consequence, these indicators should be viewed from a wider context. The scope of this policy must also be given appropriate consideration when analyzing these factors to determine potentially fraudulent or corrupt conduct.
3. Further, these indicators should not be taken to be exhaustive or definitive as they are only a guide. Please contact the Legal Department should you need further guidance with these indicators.

### **Work Practices**

- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured business environment
- Excessive variations to budgets or contracts
- Bank reconciliations are not maintained or cannot be balanced
- Excessive movements of cash funds
- Unauthorized changes to systems or work practices
- Lost assets
- Absence of controls and
- Lack of clear financial delegation

### **Employee Behavior**

- Refusal evasion or excessive delays in producing files minutes or other records
- Unexplained absences
- Gambling while at work
- Borrowing money from fellow employees while at work
- Placing undated or post-dated checks in petty cash
- Personal creditors appearing at the workplace
- Covering up inefficiencies
- Excessive turnover in any specific position
- Employees with outside business interests or other jobs that conflict with their duties
- Signs of excessive drinking or drug abuse
- Managers bypassing subordinates
- Subordinates bypassing managers

- Secretiveness
- Marked character changes
- Excessive or apparent total lack of ambition
- Excessive control of records by one employee and
- Refusal to comply with normal rules and practices

## ANNEX C - HYPOTHETICAL EXAMPLES OF FRAUD

The following items are presented to illustrate some hypothetical examples of fraudulent conduct. They are presented to assist Company personnel in maintaining awareness of potential circumstances where such behavior may occur. As with the indicators of fraud, the list is neither definitive nor exhaustive.

- An employee responsible for arranging advertising, awards graphic design contracts to a company he and his wife own or have a substantive interest in or awards contracts to acquaintances (or corporations associated with acquaintances) without the standard procedures and processes being observed.
- Several laptops are delivered to a building incorporating a number of IT departments and the laptops 'disappear'. The signature on the delivery docket, verifying that the goods were delivered, is illegible.
- An employee obtains employment under false pretences by falsely claiming to have the required qualifications.

Judgment should be exercised in considering potentially fraudulent conduct. In some circumstances, a one-off instance may constitute fraudulent conduct. In other circumstances, one-off instances of some behavior may not be considered fraudulent conduct, however, ongoing recurrences of that behavior that become material or serious in nature will be regarded as potentially fraudulent behavior.