

ValueClick, Inc.

Code of Ethics and Business Conduct

TABLE OF CONTENTS

OVERVIEW 1

THE CODE OF ETHICS AND BUSINESS CONDUCT.....2

 A. SCOPE AND RAMIFICATIONS 2

 B. CONFIDENTIALITY 3

 C. CONFLICT OF INTEREST 5

 D. COMPANY COMMUNICATIONS POLICY AND REGULATION FD 6

 E. DRUGS AND ALCOHOL..... 7

 F. ENTERTAINMENT, RECEIVING AND PROVIDING GIFTS..... 7

 G. POLICY AGAINST DISCRIMINATION 7

 H. POLICY AGAINST HARASSMENT 7

 I. COMPLAINT PROCEDURE FOR ACCOUNTING IRREGULARITIES AND ANY
 FRAUDULENT ACTIVITY 8

 J. SECURITIES TRADING 9

 K. ELECTRONIC COMMUNICATON..... 9

 L. DOCUMENT RETENTION POLICY 12

 M. RECORDS AND ACCOUNTING INTEGRITY 13

OVERVIEW

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 Code of Ethics and Business Conduct (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, officers, agents, and consultants 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 nine (9), 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.

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.

THE CODE OF ETHICS AND BUSINESS CONDUCT

A. 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 that violates the rules and standards embodied in the Code, that interferes with the Company's operations, that brings discredit to the Company, or that is offensive to the Company's customers or an employee's fellow employees, is not 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 federal law;

- employee harassment, whether it be relating to race, religious creed, color, age, sex, sexual orientation, national origin, ancestry, religion, marital status, medical condition as defined under State law, disability (sensory, mental or physical), HIV or AIDS, military service, arrest and conviction records, or any other category protected by federal, state or local 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 Company property or of another individual's property, or the failure to report any knowledge of theft; and
- falsifying any Company record or report, books of account, records, reports and financial statements, including Travel and Expense Reports and time sheets.

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 subject to the applicability of any governing law or contract of employment. 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 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.

Waivers of this Code will be granted only in exceptional circumstances. Any waivers of the Code for executive officers or directors may only be granted by the Board of Directors after disclosure of all material facts by the individual seeking the waiver and will be disclosed promptly to stockholders.

B. CONFIDENTIALITY

As an employee, you may have access to proprietary and confidential information concerning the Company's business 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 that 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.

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, unauthorized or unnecessary combing of the Company's computers or files for information without appropriate consent is a violation of the Company's policy regarding confidential and proprietary information. Such violations are not limited to "hacking" or similar acts but also include unauthorized review of another's computer that might be accessible to you in any way.

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.

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 existing or prospective customers or clients. Company records, reports, data, software and documents are confidential and employees are not permitted to disclose or release them to persons who are not directors, officers or employees of the Company, remove them or make copies of them, in whole or in part, without prior written approval of your 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 should 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. Inappropriate inquiries may include inquiries from investors, analysts or representatives of the media.

In addition, employees owe a continuing obligation of confidentiality after leaving the Company's employment, including compliance with the Company's Confidentiality 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.**

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 the Compliance Officer.

No current or former employee shall disclose any attorney-client privileged information or any attorney work product material without the prior written consent of the General Counsel of the Company (or another officer designated by the General Counsel).

Any violation of this policy on confidentiality will be grounds for disciplinary action, up to and including, immediate termination of employment, in addition to any other remedies available at law.

C. CONFLICT OF INTEREST

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. 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.

1. 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.
2. 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.
3. 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.
4. Borrowing from or lending to customers or suppliers.
5. Acquiring or having an interest in real estate that the Company owns or proposes to acquire.

6. Using Company assets, labor, or information other than for the Company's benefit or the legitimate business purposes of the Company.

7. Consulting, owning, operating or having an affiliation or controlling interest in an advertiser, publisher, affiliate or performance marketing business that is revenue generating.

Each director, officer, employee, and independent contractor must take every necessary action to comply with these guidelines and to disclose any actual or potential conflicts.

Violations of this conflict of interest policy may result in disciplinary action, up to and including termination.

D. COMPANY COMMUNICATIONS POLICY AND REGULATION FD

ValueClick is committed to consistency in its communications with others and to compliance with all applicable law. To achieve this goal, all contact with investors, analysts and members of the media should be handled by the appropriate corporate communications officer. Employees of ValueClick should direct any and all inquiries from investors, analysts or members of the media, including requests for information and interviews, to the Company's Chief Administrative Officer or Director of Corporate Communications. Employees who may be exposed to media contact, for example when attending conferences or making presentations, should be aware that ValueClick's standard corporate policy is not to comment on rumors or speculation regarding its activities. All inquiries from regulatory authorities or government representatives should be referred to the Chief Administrative Officer, Chief Financial Officer or the General Counsel.

In addition, senior management, investor relations professionals and others at ValueClick who regularly communicate with securities market professionals ("FD Persons") and holders of ValueClick securities must comply with Regulation FD ("Reg FD") promulgated by the Securities and Exchange Commission. Reg FD provides that whenever any FD Person discloses material, non-public information to certain persons (generally, securities market professionals and holders of ValueClick securities who may well trade on the basis of the information), ValueClick must also disclose that information to the general public either simultaneously (for intentional disclosures) or promptly (for inadvertent disclosures). It is the Company's policy to disclose material, non-public information on a broadly disseminated basis at a time deemed appropriate by the Chief Executive Officer and the Chief Administrative Officer. Only spokespersons approved by the Company's Chief Executive Officer and Chief Administrative Officer are permitted to disclose material, non-public information and to speak on behalf of the Company with respect to material information. **No other employee is authorized to disclose material, non-public information or to speak on behalf of the Company with respect to material information.** ValueClick's complete Company Communications Policy entitled "ValueClick, Inc. Information Disclosure Policy" dated September 2003, can be found by contacting the Company's Director of Corporate Communications or by reviewing it on the Company's intranet.

E. DRUGS AND 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.

F. ENTERTAINMENT, RECEIVING AND PROVIDING GIFTS

ValueClick will obtain, and also provide, goods and services to be used in its business based on service, quality and other relevant business considerations. Accordingly, decisions relating to the procurement and provision of goods and services should always be free from even the appearance of impropriety specifically, that favorable treatment was sought, received or given as the result of furnishing or receiving gifts, favors, hospitality, entertainment or other similar gratuity. The giving or receiving of anything of value for the express purpose of inducing such decisions is prohibited.

The payment of ValueClick funds to any officer, employee or representative of any customer or supplier in order to obtain any benefit is strictly prohibited. The competitive appeal of the Company's services and products must be based on their quality, price and other legitimate attributes recognized in the marketplace.

G. POLICY AGAINST DISCRIMINATION

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.

H. POLICY AGAINST HARASSMENT

The Company 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 occasional compliments 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 State law, disability (sensory, mental or physical), HIV or AIDS, military service, arrest and conviction records, or any other category protected by federal, state or local 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 immediately contact either the Company's General Counsel or the Vice President of Human Resources. 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 immediately. If the circumstances are such that an employee does not feel comfortable reporting the incident to his or her department manager, he or she may report it to another Compliance Officer. Any harassment reported to a manager must be reported by that manager to either the General Counsel or the Vice President of Human Resources.

This initial report 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 discharge. 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.

The Company accepts no responsibility for harassment of one employee by another employee. 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.

I. COMPLAINT PROCEDURE FOR ACCOUNTING IRREGULARITIES AND ANY FRAUDULENT ACTIVITY

The Sarbanes-Oxley Act of 2002 made a number of significant changes to federal regulation of public company corporate governance and reporting obligations. In accordance with the Act and Nasdaq requirements, ValueClick has established an accounting ethics complaint procedure for all employees of the Company and its subsidiaries. The complaint procedure is for employees who may have concerns regarding perceived accounting, internal accounting controls and auditing irregularities. If an employee feels that he or she has a concern or complaint, the procedure for expressing such concern or complaint is as follows:

- First the employee should raise his or her concern or complaint with a member of the Company's Disclosure Committee. The Disclosure Committee consists of Sam Paisley, the Company's Chief Administrative Officer, Jeff Pullen, the Company's Chief Operating Officer, Scott Ray, the Company's Chief Financial Officer, John Pitstick, the Company's Vice President of Finance and Scott Barlow, the Company's Vice President and General Counsel.
- If the employee is not satisfied that his or her concern or complaint has been appropriately addressed by the Disclosure Committee, the employee should then raise their concern with Jim Zarley, the Company's Chief Executive Officer.
- If the employee is not satisfied that his or her concern or complaint has been appropriately addressed by Mr. Zarley, the employee should then raise their concern or complaint with David Buzby, the Chairman of the Audit Committee of the Company's Board of Directors. Mr. Buzby can be reached by email at dbuzby@earthlink.net and by telephone at (415) 947-1050.

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 an ethical concern or complaint.

J. SECURITIES TRADING

All employees are responsible for reviewing, understanding and complying with ValueClick's Second Amended and Restated Policy on Insider Trading and Unauthorized Disclosure, as adopted by the Company's Board of Directors on May 23, 2002 (the Company's "Trading Policy"). ValueClick's Trading Policy is available in print form, as well as on the Company's intranet.

K. 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 explicit requirements set forth below.

You are required to use your access 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 e-mail 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, just as you would in any other business dealings. 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.

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 World Wide Web site visit, each chat, newsgroup or e-mail message and each file transfer into and out of our internal networks. 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 stored in private areas (of any form of electronic communication) 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 or 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 facilities 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. Such misuse of the Company's electronic communication facilities is subject to appropriate disciplinary action, including, but not limited to, dismissal from the Company.

User IDs and passwords help maintain individual accountability for electronic communication usage. Any employee who obtains a password or ID must keep that password confidential. Company policy prohibits the unauthorized sharing of user IDs or passwords.

Employees learning of any technical misuse of the electronic communications systems should notify their Department Manager. Employees experiencing technical or functional problems should notify the IT Department. Employees aware of other misuses (i.e., messages dealing with sexual harassment, racial slurs, etc.), are encouraged to notify the appropriate Compliance Officer or Human Resources personnel.

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 if 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 by litigation or other reason. 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 until you obtain reasonable assurances as to confidentiality.

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

Even in the case of the 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. 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 that 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 networks. Any employee who attempts to disable, defeat or circumvent any Company security facility may be subject to summary dismissal.

Internet 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.

Software Copyrights

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.

Security

Employees are provided passwords to access the Company's systems and electronic communication tools. 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.

L. DOCUMENT RETENTION POLICY

All business records should be retained for not more than one (1) year after the calendar year in which they are prepared or acquired, unless disposition is governed by other practices as specified below:

- 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;
- Electronic mail messages that remain in a user's inbox, deleted items, or sent mail folders are presumed to have no business value and will be automatically deleted after thirty (30) days;
- 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, who shall consult with intellectual property counsel in connection with patent or other intellectual property-related records;
- Accounting and financial documents are governed by policies created by the accounting department;
- Records containing personal information of employees should be retained for four years from the time the record is created unless otherwise directed by the Human Resources office;
- Sales contracts, purchase orders, leases, releases, agreements, and other contracts are retained for a period of (4) four years after the calendar year in which the performance of the contract or other obligation was completed;

Where possible, file purging will be done automatically at regular intervals. Otherwise, all personnel should review their records 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.

M. RECORDS AND 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.

COMPLIANCE CONTACT INFORMATION

In addition to the Disclosure Committee listed herein in section I, employees may contact one or both of the individuals listed below in the appropriate circumstances as described in the foregoing Code.

Outside Compliance Attorney:

Brad Weirick, Gibson, Dunn & Crutcher LLP, bweirick@gibsondunn.com, Phone = 213-229-7765

Audit Committee Chairman:

David Buzby, dbuzby@earthlink.net, Phone = 415-947-1050

EMPLOYEE ACKNOWLEDGEMENT AND ACCEPTANCE

I understand that the ValueClick, Inc. Code of Ethics and Business Conduct (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.