CODE OF CONDUCT SUMMARY

PCG has a comprehensive Code of Conduct that addresses PCG's expectations in a variety of employment situations. The Code reflects PCG's high ethical expectations for how its business is conducted. The Code applies to all individuals who work for PCG, including contractors or employees assigned to PCG through temporary employment agencies. The following is a summary of some of the key provisions of the Code that could arise during your employment with PCG:

Conflicts of Interest: If any matter comes before you at PCG relating to you or a family member, you must immediately disclose the conflict to your supervisor. For example, if you are reviewing a file in which your name appears, you must notify your supervisor and refrain from any further action on that file until you hear from your supervisor.

Sexual Harassment: PCG maintains a workplace that is free of sexual harassment and discrimination. You may not make unsolicited or unwelcome sexual conduct involving anyone at PCG. If you are the recipient of unsolicited and unwelcome sexual advances or other improper conduct, you should report the incident immediately to Human Resources.

Gifts: PCG discourages its employees from offering or accepting any gifts from clients or companies that do business with PCG. If offered such a gift, you must report the gift and its value to your supervisor.

Political Activity: You may engage in political activity outside of your PCG work schedule and work location that does not conflict with PCG's business. You may not use any PCG resources for your political activities.

Integrity of Time Sheets: You must maintain accurate time sheets that correctly reflect the time that you spend on particular projects for PCG.

Workplace Health and Safety: PCG is committed to maintaining a work environment that is free of health and safety hazards. Weapons, illegal drugs, alcoholic beverages, smoking and other tobacco products are prohibited at PCG work locations. Immediately report any hazardous situation to your supervisor.

Appearance: PCG maintains a professional business image for its clients. You are expected to wear appropriate clothing to work that is consistent with the PCG Dress Code for your office. Your supervisor can provide guidance on what clothing is appropriate for your office.

Electronic Communications: PCG may provide you with communications equipment and other resources to perform your work responsibilities. You must use PCG equipment and resources primarily for work purposes and keep personal use to a minimum so that it does not interfere with your PCG responsibilities.

Departing Employees: You may not disclose to anyone any information that you acquired at PCG that is confidential or that relates to PCG's internal business operations. Prior to departure, you must return all equipment and work-related files that you acquired at PCG.

For any questions or concerns, please contact PCG's Governance, Risk and Compliance (GRC) Officer at (617) 717-1151 or Chief Human Resource Officer at (617) 426-2026, ext. 1128. You may also utilize the confidential **PCG Compliance Hotline** at (617) 717-1400 (dial *67 first should you prefer your call to remain anonymous), or compliance@pcgus.com. More information on the Code of Conduct and Compliance Hotline can be found on PPM.

NON-DISCRIMINATION AND NON-HARASSMENT POLICY

PCG is committed to a work environment free from all forms of discrimination and unlawful harassment, including sexual harassment. This policy applies to the working relationships between PCG employees and applicants, contractors, customers, vendors, or others for whom contact is necessary for employees to perform their job duties and responsibilities.

Policy Statement

It is the policy of PCG to provide a workplace which gives every employee an equal opportunity to succeed, regardless of race, color, religious creed, sex, gender, marital status, age, sexual orientation, gender identity, national or ethnic origin, citizenship status, military service, disability or disabling conditions, or any other protected status. This policy applies to all aspects of employment, including work environment, hiring, training, performance reviews, promotions, discipline, and termination.

This policy also applies to all work-related settings, activities and communications (to include electronic, written and oral) whether inside or outside the workplace, and includes client sites, business trips, and business-related social events. PCG's property (telephones, copy machines, facsimile machines, computers, and computer applications such as e-mail and Internet access) may not be used to engage in conduct which violates this policy. PCG's policy against harassment covers employees and other individuals who have a business relationship with the firm, such as subcontractors and vendors.

PCG will not tolerate any form of unlawful discrimination or harassment in the workplace.

PCG reserves the right to view or monitor other internet forums such as social networking Web sites, blogs and other online communication tools to ensure that employees are not in violation of this policy. PCG also has an expectation that employees will represent themselves, other employees and PCG in an appropriate and professional manner. Employees are expected to express workplace issues through designated internal channels to reach an appropriate resolution.

While this policy sets forth PCG's goal of promoting a workplace that is free of unlawful discrimination and harassment, it is not designed or intended to limit PCG's authority to discipline or take remedial action for workplace conduct which the company deems unacceptable, regardless of whether that conduct violates the policy.

Sexual Harassment

Sexual harassment is offensive, affects morale, and, as a result, interferes with our work as a team. Sexual harassment can result from sexual conduct directed towards either male or female employees and can include sexual advances, requests for sexual favors, or verbal or physical conduct of a sexual nature. Sexual Harassment also includes situations when:

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

It is not possible to define precisely the type and frequency of sexual conduct that will constitute an intimidating, hostile, or offensive working environment. PCG, therefore, reserves the right to respond to and prohibit any sexual conduct in the workplace. The type of conduct that is prohibited includes, but is not limited to, verbal abuse or insults of a sexual nature, sexual jokes or other references of a sexual nature, display or circulation of sexually degrading pictures or other materials, inquiry regarding another employee's sexual experiences or activities, and other similar offensive conduct.

Hostile Work Environment

It also can be unlawful to have conduct in the workplace that denigrates or shows hostility or aversion towards an individual because of his or her race, color, religious creed, sex, gender, marital status, age, sexual orientation, gender identity, national or ethnic origin, citizenship status, military service, disability or disabling conditions, or any other protected category (or that of the individual's relatives, friends, or associates) that (1) has the purpose or effect of creating an intimidating, hostile, humiliating, or offensive working environment; (2) has the purpose or effect of unreasonably interfering with an individual's work performance.

It is not possible to know specifically the type or frequency of conduct that may constitute discriminatory harassment based on an individual's race, color, religious creed, sex, gender, marital status, age, sexual orientation, gender identity, national or ethnic origin, citizenship status, military service, disability or disabling conditions, or any other protected status. PCG therefore reserves the right to address and eliminate any conduct that is demeaning or derogatory to or stereotyping of any protected class. Examples of prohibited conduct include, but are not limited to: epithets, slurs, negative stereotyping, jokes, or threatening, intimidating, or hostile acts, and/or written or graphic material that denigrates or shows hostility towards an individual or group that is circulated in the workplace or placed anywhere on PCG's premises such as on an employee's desk or workspace or on PCG's equipment or bulletin boards.

It also is the policy of PCG to encourage employees to come forward to report any conduct in or affecting the workplace, and/or to cooperate in any investigation of possible harassment.

Retaliation

This policy and the law prohibit retaliation against any employee who reports possible harassment or discrimination or cooperates with an investigation of possible harassment or discrimination. PCG will not tolerate any retaliatory conduct towards an individual because that person participated in this process.

Process for Investigating Allegations of Harassment

If an employee at PCG believes that he or she has been subjected to conduct that may be harassment, the employee is strongly encouraged to inform his or her supervisor and one or both of the following persons. If the employee for any reason prefers to do so, they may report the incident to the President, or they may submit the report on an anonymous and confidential basis by contacting the PCG Compliance Hotline listed below.

Contacts	**Telephone Number**
Chief Human Resource Officer	(617) 717-1128
Governance, Risk and Compliance Officer	(617) 717-1151

PCG Compliance Hotline - (617) 717-1400 (Note: callers have the option to remain anonymous by dialing *67 first); compliance@pcgus.com

Any reported incident will be promptly and thoroughly investigated. While each investigation will proceed as the particular circumstances warrant, an investigation usually involves an interview with the employee making the report and interviews with persons identified as witnesses or otherwise having knowledge of the incident or conduct. The firm and all those who participate in the investigation shall maintain as much confidentiality as possible under the circumstances, while ensuring an effective investigation. Also, all persons will be informed that it can be unlawful and PCG will not tolerate any form of retaliation directed towards an individual who makes a complaint or who participates or cooperates in an investigation.

If as a result of the investigation it is determined that any individual engaged in conduct that may be harassment, appropriate remedial or disciplinary action will be taken. Depending on the nature, severity and frequency of the conduct, such actions may include, but are not limited to: eliminating contact between the employee involved in the incident, mandated training and/or counseling, demotion, or termination of employment.

The importance of this policy cannot be emphasized enough. An environment free of sexual and other harassment is fundamental to the culture of PCG. While we hope that any employee who believes that he/she has been subjected to harassment or retaliation will immediately bring the matter to the attention of managers and/or Human Resource staff, PCG employees also have the right to contact the Equal Employment Opportunity Commission (EEOC). Their web site, www.eeoc.gov provides details relative to how to file a charge and lists the locations of local field offices. Employees also have the right to file a charge with their State's local civil rights agency. This contact information can generally be found on each state government's web site.

Drug and Alcohol Policy

Illegal or inappropriate drug and alcohol use is detrimental to the safety and productivity of employees. Using, possessing, or being under the influence of alcohol or any illegal drug while engaged in PCG business, while on PCG premises, or while operating a vehicle or machine leased or owned by PCG is prohibited. PCG employees or job applicants may be required to submit to a drug test if called for by a client contract or if Management has a reasonable suspicion of a violation of federal or state law, policy, or client contract. Employees convicted of any criminal drug violation while working for PCG must report such conviction to the Chief Human Resource Officer within five calendar days.

Employees who must use medication, whether prescription or non-prescription, that might impair their ability to perform their duties should inform their supervisor as follows:

1. That they are taking such medication;

2. Of any possible side effects of the medication that could affect their safety or job performance (e.g., drowsiness or impaired reflexes); and

3. The expected duration of their use of such medication.

If use of such medication could cause safety or job performance problems, PCG may grant the employee PTO or temporarily assign him or her to different duties.

From time to time, PCG may sponsor events or gatherings where alcohol is served. Alcohol may be served at these events only with the prior written approval of the Chief Human Resource Officer or the President. In no instance, however, may an employee consume so much alcohol that it impairs his or her ability to act in a responsible and professional manner.

Violation of this policy will lead to disciplinary action, up to and including immediate termination.

To the extent that you have any questions regarding the application of this policy, please contact the Chief Human Resource Officer or the GRC Officer for further clarification.

Security and Confidentiality POLICY

PCG is committed to ensuring the security and confidentiality of data that is entrusted to it by its clients and others, including "Protected Health Information" (PHI) under the Health Insurance Portability and Accountability Act ("HIPAA"), "education records" under the Family Educational Rights and Privacy Act ("FERPA"), and other data that is confidential under other applicable laws, regulations, contracts, or ethical standards.

Additionally, PCG is committed to safeguarding its confidential business information and trade secrets. The protection of business information and trade secrets is vital to the interests and the success of PCG. Such information includes, but is not limited to, the following examples:

- PCG security codes
- Personnel and/or compensation data
- Computer processes, programs, codes, and/or proprietary software
- Customer lists and/or preferences
- Dollar value and scope of services of any PCG contract
- Customer confidential and/or financial information
- Company financial information
- Marketing strategies
- Pending projects and proposals, such as sales
- Technological data and/or prototypes

All PCG employees are expected to read, understand, and comply with this policy. For purposes of this policy, the term "security" relates to protection of confidential data from internal and/or external threats. The term "confidentiality" relates to protection of confidential data from improper use or disclosure.

PCG employees may not use confidential data, as defined in its Data Classification Standards, for any purpose other than performing their PCG work responsibilities. Employees may not share or otherwise disclose, via any communication vehicle, confidential information acquired at or on behalf of PCG to anyone outside of PCG. Employees who improperly use or disclose confidential information either during or after employment will be subject to disciplinary action, up to and including termination of employment and legal action, even if they do not actually benefit from the disclosed information. An employee who is uncertain whether particular information is confidential is encouraged to seek and comply with guidance from either an appropriate manager, the PCG Chief Information Security Officer, PCG Legal Counsel, or the PCG Governance, Risk and Compliance (GRC) Officer prior to any disclosure.

The protection of confidential information requires continual employee vigilance as well as awareness that the sharing of such information can occur unintentionally. Employees shall take reasonable steps to assure security in the transmission of confidential information, including the verification of mailing and e-mail addresses and telefax numbers prior to transmitting confidential information.

PCG provides employee access to confidential information on a need-to-know basis, defined as having a business need for access to information in order to carry out job responsibilities. Employees may not browse or otherwise explore confidential information beyond what is required to carry out their PCG job responsibilities.

A. Basic Principles

1. PCG will maintain and use appropriate administrative, physical, and technical safeguards to reasonably protect the security, integrity, and confidentiality of its confidential data.
2. PCG will not disclose confidential data to any employee, contractor, or other person unless that person has executed an appropriate agreement relating to the security and confidentiality of its confidential data within the past one year.
3. PCG will not use or disclose confidential data except as authorized in writing by the source of the confidential data.
4. PCG will immediately investigate any reported breach of its security and confidentiality safeguards. If a breach is confirmed, PCG will notify the source of the data, and will take appropriate steps to correct the problem and to mitigate any harm.

B. Security Systems and Information Security

1. PCG utilizes physical and electronic systems to secure confidential data. Physical systems include building access controls and other physical security controls. Electronic systems include computer passwords, firewalls, virus detection software, and encryption. Employees are prohibited from bypassing these systems.
2. The Chief Information Security Officer maintains detailed procedures for PCG electronic security systems, including how the HIPAA Security Rule is addressed, and is responsible for electronic security awareness and training.
3. The Information Security program maintains detailed policies and standards that must be reviewed and understood by anyone working for PCG. All of the PCG workforce has responsibilities as documented in both this and all Information Security policies/standards.

C. Project Requirements

For each project that involves the use of confidential data, the Project Manager is responsible for ensuring and documenting compliance with the security and confidentiality requirements that are contained in: (a) the contract under which the data is made available to PCG; and (b) this policy.

1. **Required project documents.** For each project that involves the use of confidential data, required project documents include the following: (a) this policy; (b) a HIPAA "business associate" agreement or other written agreement with each source of PHI data, pertaining to the use and disclosure of that confidential data; (c) agreements with any project contractors and other non-PCG individuals or entities relating to the use or disclosure of confidential data that they did not provide; and (d) the confidential data itself. The client contract does not govern the use of confidential data other than the data that is provided by the client.
2. **Security of Electronic Data.** The Project Manager will consult as necessary with the Chief Information Security Officer with respect to the security of confidential data that is held or used in electronic form. This includes encryption, the availability of secure data storage facilities, the use of computers and laptops, and the disposition of confidential data at the end of a project (pursuant to the project record retention plan).
3. **Security of Non-Electronic Data**. The Project Manager will consult as necessary with the appropriate office manager and Practice Area Director with respect to the security of confidential data that is held or used

in non-electronic form. This includes ensuring the availability of secure data storage facilities and the disposition of the confidential data after the expiration of the contract (pursuant to the corporate record retention plan or project specific requirements).

4. **Use of Confidential Data.** Confidential data may be used only for the specific purpose(s) for which it was made available to PCG, as documented in a HIPAA Business Associate Agreement or other written agreement with the entity that made the data available, or as may be required by law. To the extent that confidential data is used or disclosed "as required by law," rather than pursuant to the documented agreement with the source of the confidential data, that use or disclosure will be discussed in advance with PCG Legal Counsel and documented in the project file.
5. **Access to Confidential Data.** Access within PCG to confidential data is limited to PCG employees and contractors who require such access for purposes of a project for which the data was provided. Confidential data must not be discussed or made accessible outside a secure environment.
6. **Transmission of Confidential Data**. Confidential data may be transmitted only in a way that protects its security and confidentiality. For non-electronic data, this includes the use of a delivery service that allows packages to be tracked. For electronic data, this includes encryption.

D. Training

1. **Training.** PCG will require anyone working on its behalf to take appropriate training relating to the security and confidentiality of confidential data. To the extent appropriate, the training will focus on new developments and use actual scenarios. Everyone is required to complete such training prior to receiving access to PCG's confidential data.
2. **Subcontractors and contractors.** Training requirements may apply as well to subcontractors and other PCG contractors, depending on the nature of their work.

E. Personnel Responsibilities

Anyone working for PCG has responsibilities relating to this policy.

1. **Everyone working on behalf of PCG** is responsible for understanding the policy, complying with the policy, and reporting violations of the policy to an appropriate supervisor, the Governance, Risk and Compliance (GRC) Officer or PCG Legal Counsel. Everyone is required to read and acknowledge this policy before having access to confidential data, and to sign an acknowledgement of this policy on at least an annual basis. The executed acknowledgement form will be kept on file with PCG HR.
2. **Project Managers** are responsible for ensuring compliance with the policy on the project, including by any temporary employees and contractors. In the event of a breach of security or confidentiality, the Project Manager is responsible for notifying the GRC Officer and PCG Legal Counsel and for taking the steps recommended by GRC and Legal Counsel to notify the source of the confidential data, to correct the problem, and to mitigate any harm.
3. **The Governance, Risk and Compliance Officer** is responsible for implementing and maintaining the compliance program, for addressing reports of violations, and for reporting directly to senior management on reported violations and other aspects of the compliance program. The GRC Officer will also answer employee questions regarding compliance or ethics issues.
4. **The Information Security Officer** is responsible for implementing and maintaining the information security program and for implementing measures to secure PCG's data and assets as required by business needs, contracts, and applicable laws and regulations.

F. Reports of Violations

1. **Reports.** Employees are to report violations of the policy to their supervisors, who will promptly notify GRC and PCG Legal Counsel, or directly to GRC or PCG Legal Counsel.
2. **Confidentiality.** Reports to the GRC Officer may be made on a confidential basis by calling the PCG Compliance Hotline, at (617) 717-1400 (callers should dial *67 first if they prefer the call to be anonymous), or via e-mail to compliance@pcgus.com.
3. **Response.** The GRC Officer will log each report of non-compliance, will address each report, and periodically will report to senior management on each violation and its disposition.
4. **Retaliation.** Employees making a good faith report of non-compliance will not be retaliated against on account of the report.
5. **Documentation.** Reports of violations relating to a project will be documented in writing, and will be included in the project file as a project document along with documentation of the corrective actions taken, with an appropriate level of documentation also sent to the Corporate Chief Human Resource Officer.

G. Evaluations

1. Adherence to this policy, including the fulfillment of training requirements and the timely reporting and proper handling of violations, will be elements of employee performance evaluations.
2. The exit interview for employees leaving PCG will ask whether the employee was aware of any violations of this policy, and any reports will be investigated by the GRC Officer and Legal Counsel. The exit interview will also remind anyone leaving PCG of their responsibilities as stated in this policy.

H. Monitoring

The GRC Officer, Chief Information Security Officer and Legal Counsel will monitor the operation of this policy, and will recommend and implement any necessary modifications.

I. Documentation

PCG will retain appropriate documentation relating to this policy, including the project documentation, the training acknowledgments, and the reports of violations and corrective actions.

The confidentiality obligations explained in this policy continue after termination of an employee's employment for any reason.

ELECTRONIC COMMUNICATIONS POLICY

All firm communications systems, including E-mail and voicemail, are provided as communication tools for conducting PCG business. It is important that staff recognize that these systems are PCG property, and utilize these systems (including "All Staff" and other PCG distributions lists) for professional and business-related purposes. Employees who violate this policy will be subject to disciplinary action, which could result in termination.

Access and Disclosure
Staff and other users have no right of privacy regarding any information maintained in or on PCG's property, or transmitted or stored through PCG systems, including voicemail, E-Mail, internet access, Internet blogs, or other technical resources. This means that any message sent or received on PCG's computer systems or other technical resources is subject to investigation, search, and review by PCG in its discretion without notice. Even electronic tracks or messages that users believe they have deleted remain subject to PCG's review.

Password Security
The security and protection of individual passwords is a prime responsibility of the individual owner of the password. Therefore, if something is authored out of a password-protected system, the presumption will be that the owner of the password authored it.

PCG does not authorize use of passwords to gain access to another user's information or communications. It is a violation of firm policy for any user, including firm administrators and supervisors, to use firm communications systems to satisfy curiosity about the affairs of others, with no business reason for obtaining access to the files or communications of others.

Confidential Information and Privileged Communications
Users of PCG communications systems must adhere to PCG's Confidentiality Guidelines in sending or forwarding information confidential to the firm or its clients. Users should proceed with caution in sending or forwarding confidential information on firm communications systems because incorrect or inadvertent distribution can occur more easily than with some other means of communicating information. Confidential information that must be sent via the Internet must always be encrypted, for security purposes.

Copyrighted Information
Use of PCG's communications systems to copy or transmit documents, software, information, or other materials protected by the US copyright laws is prohibited unless permitted by license or permission from the copyright owner.

Internet Use
PCG provides Internet access to its employees for business purposes. Employees may utilize such access for personal purposes on occasion, so long as such access does not interfere with the employee's work. Employees are prohibited from accessing, transmitting, or printing any information from any Web site if the content is offensive or would violate any PCG policy. PCG monitors internet access and may spot check Web sites visited by employees. Any user knowingly introducing a computer virus into the PCG communications systems will be subject to disciplinary action.

Other Issues

PCG communications systems may not be used to engage in any communication that is unlawful or in violation of firm policy, including, but not limited to, communication that is defamatory, discriminatory, defaming, obscene, or in violation of PCG's Equal Opportunity or Non-Discrimination and Non-Harassment Policies. In particular, communications that inappropriately target protected classes or are demeaning or offensive will not be tolerated. This includes, but is not limited to, messages, jokes, stories, or pictures that offensively reference someone's age, race, sex, national origin, disability, sexual orientation, gender identity or religious beliefs.

Usage of PCG communications systems is audited in message units. Excessive personal use is subject to disciplinary action.

PCG does not authorize the use of firm communications systems to solicit or conduct business other than the business of the firm. It is a violation of PCG policy to use firm communications systems to solicit or advocate for issues, causes or organizations of any kind when such solicitation or advocacy is deemed personal in nature and not recognized as furthering the reputation and interest of PCG.

POLICIES AND PROCEDURES ACKNOWLEDGEMENT
TEMPORARY EMPLOYEE OR CONTRACTOR

Please sign this acknowledgement page and forward to your agency contact prior to your first day of work with Public Consulting Group, Inc. (PCG).

This certifies that I have received, read and accept the following PCG corporate policies.

CODE OF CONDUCT SUMMARY
NON-DISCRIMINATION AND NON-HARASSMENT POLICY
DRUG AND ALCOHOL POLICY
SECURITY AND CONFIDENTIALITY POLICY
ELECTRONIC COMMUNICATIONS POLICY

I understand that these policies are not expressed or implied terms of a contract of employment, and can be changed at any time at the discretion of PCG.

Name (Signature) _____ Date _____

Name (Printed) _____