



## FRAUD POLICY

### **Purpose and Background**

PSC is committed to the highest standards of moral and ethical behavior. The purpose of PSC's Fraud Policy is to foster an environment that promotes awareness to fraudulent practices and facilitates the development of controls to aid in the prevention and detection of fraud. Fraudulent activity of any kind, including acts where PSC may benefit, is expressly forbidden. This policy establishes the procedures and responsibilities for reporting and resolving instances of known or suspected fraudulent acts.

The framework of this policy embodies three fundamental principles:

1. Create and maintain a *culture* of honesty and high ethics;
2. *Evaluate* the risks of fraud and implement the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud; and
3. Develop an appropriate *oversight* process.

### **Scope of Policy**

In broad terms, fraud refers generally to any intentional act committed to secure an unfair or unlawful gain. For the purposes of PSC's Fraud Policy, it is defined as an intentional act to deprive PSC, or any individual or entity related to PSC's business, of something of value, or to gain an unfair advantage through the use of deception, false suggestions, suppression of the truth, or some other unfair means, which are believed and relied upon.

A fraudulent act may be an illegal, unethical, improper, or dishonest act including, but not limited to:

- embezzlement;
- misappropriation, misapplication, destruction, removal or concealment of funds, securities, supplies or other assets;
- forgery, alteration or falsification of documents, including checks, bank drafts or any other financial documents;
- false claims by employees, vendors or others associated with PSC;
- theft or destruction of any asset including, but not limited to, money, tangible property, trade secrets or intellectual property;
- profiteering as a result of insider knowledge of PSC activities;
- Inappropriate use of computer systems, including hacking and software piracy, as well as the intentional alteration, destruction or manipulation of data;
- bribery, rebate or kickback;
- conflicts of Interest;
- misrepresentation of facts;
- improper reimbursement for non-company or unauthorized expenses or reimbursement of expenses more than once;
- intentional non-compliance with applicable laws, rules and regulations;
- intentional failure to provide full, fair, accurate, timely, and understandable disclosure in reports and documents.

### **Duties and Responsibilities**

Management is responsible for setting the appropriate tone of intolerance for fraudulent acts by displaying the proper attitude toward complying with laws, rules, regulations, and policies, including ethics policies. In addition, management should be cognizant of the risks and exposures inherent in their area of responsibility and should establish and maintain proper internal controls that will provide for the security and accountability of the resources entrusted to them.

Additionally, management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and for ensuring a culture and environment that promotes honest and ethical behavior.

All employees of PSC who have a reasonable basis for believing fraud or other wrongful acts have occurred have a responsibility to report such incidents to their immediate supervisor. If notifying the supervisor is not possible



because of absence or because you believe your supervisor may be involved, you should notify the next highest supervisor or the PSC Internal Audit Department directly. All supervisory personnel informed of suspected fraud or other wrongful acts must immediately notify the PSC Internal Audit Department. All information will be treated confidentially.

A confidential Hotline number is available as well to report suspected inappropriate behavior. The PSC Ethics/Fraud Hotline number is **1.800.241.5689**. The Hotline should be used to report any suspected improper behavior including:

- Fraudulent activity
- Ethics violations
- Environmental non-compliance
- Safety concerns

### **Investigation**

PSC's Internal Audit Department shall have the primary responsibility for tracking and prioritizing suspected fraudulent activity, as well as determining whether further investigation needs to be performed. In addition, PSC's Internal Audit Department will investigate suspected fraudulent acts as defined in this policy when appropriate. Any employee who suspects dishonest or fraudulent activity should notify the PSC Internal Audit Department directly, via phone or email, or through the PSC Ethics Hotline. An employee should not attempt to personally conduct investigations and should not contact the suspected individual in an effort to determine facts or demand restitution.

PSC's Internal Audit Department will coordinate with PSC's Legal Counsel, Senior Management and other levels of management, as deemed necessary, when fraud or other wrongful acts are suspected.

Great care will be taken in the investigation of suspected improprieties or irregularities so as to avoid incorrect accusations, making statements which could provide a basis for a false accusations law suits, or alerting suspected individuals that an investigation is taking place. Accordingly, the reporting individual should **NOT**:

- contact the suspected individual to determine facts or demand restitution.
- discuss any facts, suspicions, or allegations associated with the case with anyone, unless specifically directed to do so by PSC's Internal Audit Department or PSC's Legal Counsel.

***Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/job title or relationship to PSC.***

This policy also applies to vendors, consultants, contractors, outside agencies doing business with employees of PSC, and/or any other parties with a business relationship with PSC.

- In instances where the investigation indicates the probability of criminal activity, the investigation will be turned over to PSC's Legal Counsel, who in turn may contact the appropriate law enforcement agency.
- Investigations will be completed expeditiously, but always in a thorough manner and in accordance with established procedures. It is the duty of all individuals to cooperate fully with those performing an investigation pursuant to this policy. The constitutional rights of those involved will always be observed.

Upon completion of a fraud investigation, the PSC Internal Audit Department will submit a report detailing the findings to Senior Management and other members of management, as appropriate. When deemed appropriate, the PSC Internal Audit Department may make a recommendation to refer the matter to the appropriate law enforcement and/or regulatory agencies for independent investigation. The decision to involve outside sources shall be made by PSC's Senior Management in conjunction with PSC's Legal Counsel.

### **Confidentiality**

The PSC Internal Audit Department will treat all reports of suspected fraud or irregularities, as well as all information obtained through investigation, whether received via phone, e-mail or through the Ethics Hotline, with the strictest of confidentiality. Employees may remain anonymous but are encouraged to cooperate with investigators and should provide as much detail and evidence of the suspected fraudulent activity as possible.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the PSC Internal Audit Department of PSC Legal Department.



### **Whistle Blower Protection**

No manager or person acting on behalf of the manager shall:

- dismiss or threaten to dismiss an employee;
- discipline or suspend, or threaten to discipline or suspend an employee;
- impose any penalty upon an employee; or
- intimidate or coerce an employee, in conjunction with an employee's actions to notify or cooperate with PSC's Internal Audit Department related to suspected fraudulent activity, because the employee has acted in accordance with the requirements of this policy.

The violation of this section will result in discipline up to and including dismissal.

### **Authorization for Investigating Suspected Fraud**

In the course of an investigation of suspected fraud, with proper notification of the appropriate level of management, PSC Internal Audit shall have:

- free and unrestricted access to all PSC records, premises, and facilities, whether owned or rented by PSC;
- the authority to interview employees; and
- the authority to examine, copy and/or remove all documents, electronic data, files, tapes, disks, computers, and other equipment and storage facilities on the premises without prior knowledge or consent of any individual who may use or have custody of any such items or facilities when it is within the scope of the investigation.

### **Actions**

Employees found to have participated in fraudulent acts, as defined by this Policy, will be subject to disciplinary action, up to and including termination, pursuant to personnel policies and rules. Additionally, employees suspected of perpetrating fraudulent acts may be placed on suspension during the course of the investigation. In those cases where disciplinary action is warranted, Senior Management, Human Resources and/or other appropriate personnel will be consulted prior to taking such actions. Criminal or civil actions against employees who participate in unlawful acts will be forwarded to the appropriate agency.

The employment of any employee involved in the perpetration of fraud will ordinarily be terminated. Actions to be taken will be determined without regard for past performance, position held, length of service, race, color, religion, sex, age disability, national origin or veteran status.

### **Glossary of Fraud Terms**

**Affiliate Bidding:** A condition in purchasing when multiple bids are tendered for a contract from a single company under various names to give the appearance of competition.

**Asset Misappropriation:** Involve the theft or misuse of an organization's assets. (Common examples include skimming revenues, stealing inventory, and payroll fraud)

**Bid Rigging:** In purchasing, any scheme that gives the appearance of competitive bids but is actually not competitive because the participants establish the winner before submitting bids for the contract.

**Billing Schemes:** An individual causes the victim organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

**Bribery:** To offer money in exchange for favorite treatment or to compel or influence some action. Official (government employee or elected official) bribery involves a promise for acting or withholding some official act. Official bribery (*corruption*) is unlawful in most cultures. *Commercial Bribery* is known as "facilitating payments" in some cultures and is not a crime in most cultures, although it often is against the organization's policies and procedures.



**Cash Larceny:** Cash is stolen from an organization after it has been recorded on the organization's books and records.

**Check Tampering:** The perpetrator converts an organization's funds by forging or altering a check on one of the organization's bank accounts, or steals a check the organization has legitimately issued to another payee

**Coerce:** To influence action against someone's will, usually by threat.

**Conflict of Interest:** An employee owes a duty to the employer to act in the interest of the employer (and no other) when carrying out the duties of an employer. A Conflict of Interest exists when the employee has some personal kinship, friendship, or financial interest in the transaction that may divide the employee's interests and put his duty to his employer in jeopardy.

**"Cooking the Books":** Altering the official accounts to deceive.

**Embezzlement:** Theft of money from an employer by an employee using false entries in accounting records to cover up the crime.

**Employee Account Fraud:** When employees are also customers, employees may make unauthorized adjustments to their accounts (including write-off).

**Expense Report Fraud:** Charging unauthorized or fictitious amounts on an expense report.

**Extortion:** The offer to keep from harm in exchange for money or other consideration. The demand for *Restitution* in exchange for not prosecuting a crime is a form of extortion.

**False Claims:** Claims for reimbursement by an employee or contractor for nonexistent or inflated expenses. False claims can be for business expenses or personal expenses (such as medical).

**False Credentials:** Misrepresenting education or experience or professional certification to fraudulently obtain and hold employment.

**Falsification of Financial Information:** False accounting entries, bogus trades designed to inflate profit or hide losses, and false transactions designed to evade regulatory oversight.

**Fictitious Refunds Scheme:** Preparing false documents of refunds to cover thefts of cash.

**Fictitious Sales:** A scheme to record sales to fictitious customers or fictitious sales to existing customers at the end of one period and reversing the transactions at the beginning of the next period. The purpose of the scheme is to inflate sales to create false profit statements or earn unwarranted bonuses. Excessive credit memos or sales cancellations at the beginning of an accounting period can be an indicator of this fraud.

**Forgery:** Creation of false documents or altering existing documents, especially financial instruments or other authorizations.

**Fraudulent Disbursements:** The perpetrator causes his organization to disburse funds through some trick or device (common examples include submitting false invoices or false timecards).

**"Ghost" Employees:** Fictitious employees on the payroll, for whom the supervisor or manager receives the extra paychecks.

**Inflated Inventory:** An indication of *Embezzlement* or possible theft of inventory.

**Influence Pedaling:** The offer by a government official to use their office to influence actions for a private party in return for something of value.

**Journal Entry Fraud:** Using accounting journal entries to fraudulently adjust financial statements.

**Kickback:** A payment by a vendor to an employee at the request of the employee in order for the vendor to receive favorable treatment.



**Lapping:** Stealing a customer payment then using a subsequent customer payment to cover the previous customer's account. This overlapping of payments creates a "float" of money that can be used as long as all payments are eventually posted. What usually occurs is that the lapping process builds up like a giant pyramid until it falls apart when not enough payments are available to cover the amounts owed.

**Negative Invoicing:** Using an invoice for a negative amount to cover a theft of a customer payment. The negative invoice is less noticeable than a credit memorandum and usually under less stringent control. A negative invoice is a symptom of possible theft.

**Over billing Schemes:** Padding invoices with extraneous or fictitious items. Intentional duplicate billing, such as billing two parties for the same work is also an over billing scheme.

**Out-of-Route:** Outside sales or service workers who deviate from their normal route or time schedule, such as conducting personal errands or taking excessively long coffee or lunch breaks.

**Padding Expense Accounts:** Adding extra expense items or inflating the value of legitimate expense items to obtain unwarranted reimbursements.

**Padding Overtime:** Adding extra hours to falsely inflate the payroll and earn unwarranted pay.

**Payroll Schemes:** An employee causes the victim organization to issue a payment by making false claims for compensation.

**Pilfering:** *Theft*, usually referring to theft of physical goods. In retail business, customer theft is known as *Shoplifting* and employee theft is called pilfering. Occasionally used also with theft of cash, especially petty cash or for small thefts.

**Sabotage:** Destroying or delaying some part of the business process.

**Self-Dealing** (by corporate insiders): Insider Trading, kickbacks, and/or misuse of corporate property for personal gain, and individual tax violations related to self-dealing.

**Skimming:** Cash is stolen from an organization before it is recorded on the organization's books and records.

**Subterfuge:** Masking the true nature or reason for an action.

**Theft of Proprietary Information and Trade Secrets:** Use or disclosure of confidential company information for personal gain or to the detriment of PSC.

**VOIDS:** In cashiering, ringing a "Void" to cancel a previous sale. Excessive voids may be a sign of theft.

**Worker's Compensation Fraud:** False claims for on-the-job injuries. Usually takes the Collusion of employee and unscrupulous doctors to submit false diagnoses. Back injuries (soft tissue strains) and stress are the most common ailments used in this scheme.