PC Connection, Inc.

PC CONNECTION, INC. CODE OF BUSINESS CONDUCT AND ETHICS

Applicable to All Subsidiaries

I. Purpose.

To establish uniform standards of conduct under which each of the PC Connection, Inc. family of companies will operate and transact business.

II. Application.

This Code of Business Conduct and Ethics (the "Code") sets forth legal and ethical standards of conduct for directors, officers and employees of PC Connection, Inc. and its subsidiaries (hereinafter "Company").

III. Standards of Conduct.

The Chairman and Chief Executive Officer of the Company expect that all directors, officers and employees will maintain the highest ethical standards in the conduct of Company affairs. This Code is intended to deter wrongdoing and to promote the conduct of all Company business in accordance with high standards of integrity and in compliance with all applicable laws and regulations. Each Employee will conduct the Company's business with integrity and comply with all applicable laws and regulations, and in a manner that excludes considerations of personal advantage or gain.

All employees are also expected to adhere to the rules and practices of the Company set forth in the Company's employment and personnel policies published and disseminated to employees on the Company's Worknet website, in the Company's Orientation Guidebook, or otherwise. In case of any inconsistency between this Code and those policies, this Code shall apply. If you have any questions regarding this Code or its application to you in any situation, please contact Dick Saporito in the Human Resources Department.

Compliance with the Code, Company Policies, Laws, Rules and Regulations; Obligation to Report; Prohibition against Retaliation

Every director, officer and employee of the Company is required to comply in all respects with the Code, Company policies and all laws, rules and regulations applicable to the Company wherever it does business. You are expected to use good judgment and common sense in seeking to comply with all applicable laws, rules and regulations and to ask for advice when you are uncertain about them. We also expect that any agents, consultants or representatives working on behalf of the Company will adhere to high ethical standards and will not engage in any conduct prohibited by the Code.

If you become aware of the violation of any law, rule or regulation by the Company, whether by its officers, employees, directors, or any third party doing business on behalf of the Company, it is your responsibility to promptly report the matter to Dick Saporito in the Human Resources Department.

It is the Company's desire to have the opportunity to fully address matters internally. You are therefore encouraged to report any illegal activity to the officers identified above. Illegal activities include violation of the securities laws, antitrust laws, and environmental laws or any other federal, state or foreign law, rule or regulation. If you believe that your concerns are not being reasonably addressed, you may report such violation directly to the Audit Committee of the Board of Directors.

You may file an anonymous complaint at http://www.MySafeWorkplace.com. Following an initial investigation, all bona fide complaints will be reported to the Audit Committee.

If, following report to the Audit Committee, you still believe that your concerns are not being reasonably addressed; you may report the violation to the appropriate regulatory authority. Employees, officers and directors shall not discharge, demote, suspend, threaten, harass or in any other manner discriminate or retaliate against an officer, employee, or director because he or she in good faith reports any such violation. This Code should not be construed to prohibit you from testifying, participating or otherwise assisting in any state or federal administrative, judicial or legislative proceeding or investigation.

Conflicts of Interest

Employees, officers and directors must act in the best interests of the Company. You must refrain from engaging in any activity or having a personal interest that presents a "conflict of interest." A conflict of interest occurs when your personal interest interferes, or appears to interfere, with the interests of the Company. A conflict of interest can arise whenever you, as an officer, director or employee, take action or have an interest that prevents you from performing your Company duties and responsibilities honestly, objectively and effectively.

For example, no employee, officer or director shall:

- Perform services as a consultant, employee, officer, director, advisor or in any other capacity for, or have a financial interest in, a direct competitor of the Company, other than services performed at the request of the Company and other than a financial interest representing less than one percent (1%) of the outstanding shares of a publicly-held company; and
- Use his or her position with the Company to influence a transaction with a supplier or customer in which such person has any personal interest, other than a financial interest representing less than one percent (1%) of the outstanding shares of a publicly-held company.
- Supervise, review or influence the job evaluation or compensation of a member of his or her immediate family; or
- Engage in any other activity or have any other interest that the Board of Directors of the Company determines to constitute a conflict of interest.

These examples are not meant to be an exhaustive list of situations that could create a conflict of interest. It is your responsibility to disclose any transaction or relationship that reasonably could be expected to give rise to a conflict of interest to Dick Saporito in the Human Resources Department.

Definitions

For purposes of this Code, a "close relative" means a spouse, dependent child or any other person living in the same household with the employee, officer or director. "Immediate family" means a close relative and a parent, sibling, child, mother- or father-in-law, son- or daughter-in-law or brother- or sister-in-law. A "significant customer" is a customer that has made during the Company's last full fiscal year, or proposes to make during the Company's current fiscal year, payments to the Company for property or services in excess of one (1) percent of (i) the Company's consolidated gross revenues for its last full fiscal year, or (ii) the customer's consolidated gross revenues for its last full fiscal year. A "significant supplier" is a supplier to which the Company has made during the Company's last full fiscal year, or proposes to make during the Company's current fiscal year, payments for property or services in excess of one (1) percent of (i) the Company's consolidated gross revenues for its last full fiscal year, or (ii) the customer's consolidated gross revenues for its last full fiscal year.

Insider Trading

Employees, officers and directors who have material non-public information about the Company or other companies, including our suppliers and customers, as a result of their relationship with the Company are prohibited by law and Company policy from trading in the securities of the Company or such other companies, as well as from communicating such information to others who might trade on the basis of that information. If you are uncertain about the constraints on your purchase or sale of any Company securities, or the securities of any other company that you are familiar with by virtue of your relationship with the Company, you should consult with Dick Saporito in the Human Resources Department before making any such purchase or sale.

Confidentiality

Employees, officers and directors must maintain the confidentiality of sensitive information entrusted to them by the Company or other companies, including our suppliers and customers, except when disclosure is authorized by the Company or legally mandated. Unauthorized disclosure of any confidential information is prohibited. Additionally, employees should take appropriate precautions to ensure that confidential or sensitive business information, whether it is proprietary to the Company or another company, is not communicated within the Company except to employees who have a need to know such information to perform their responsibilities for the Company.

Third parties may ask you for information concerning the Company. Employees, officers and directors (other than the Company's authorized spokespersons) must not discuss internal Company matters with, or disseminate internal Company information to, anyone outside the Company, except as required in the performance of their Company duties and after an appropriate confidentiality agreement is in place. This prohibition applies particularly to inquiries concerning the Company from the media, market professionals (such as securities analysts, institutional investors, investment advisers, brokers and dealers) and security holders.

All responses to inquiries on behalf of the Company must be made only by the Company's authorized spokespersons. If you receive any inquiries of this nature, you must decline to comment and refer the inquirer to your supervisor or to one of the Company's authorized spokespersons. Questions regarding the Company's disclosure practices should be directed to Corporate Communications.

You must also abide by any lawful obligations that you have to your former employer. These obligations may include restrictions on the use and disclosure of confidential information, restrictions on the solicitation of former colleagues to work at the Company, and non-competition obligations.

Honest and Ethical Conduct, and Fair Dealing

Employees, officers and directors should endeavor to deal honestly, ethically and fairly with the Company's suppliers, customers, competitors and employees. Statements regarding the Company's products and services must not be untrue, misleading, deceptive or fraudulent. You must not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair-dealing practice. The Company's business transactions must always be in compliance with antitrust laws and regulations.

Protection and Proper Use of Corporate Assets

Employees, officers and directors should seek to protect the Company's assets. Theft, carelessness and waste have a direct impact on the Company's financial performance. Employees, officers and directors must use the Company's assets and services solely for legitimate business purposes of the Company and not for any personal benefit or the personal benefit of anyone else. Employees, officers and directors must advance the Company's legitimate interests when the opportunity to do so arises. You must not take for yourself personal opportunities that are discovered through your position with the Company or the use of property or information of the Company.

Gifts and Gratuities

The use of Company funds or assets for gifts, gratuities or other favors to employees or government officials is prohibited, except to the extent such gifts are in compliance with applicable law, nominal in amount and not given in consideration or expectation of any action by the recipient. It is a violation of this Code to give or offer anything of value to government officials in order to influence their actions or decisions, or if doing so would negatively reflect on the Company's, or the official's, integrity or reputation.

Employees, officers and directors must not accept, or permit any member of his or her immediate family to accept, any gifts, gratuities or other favors from any customer, supplier or other person doing or seeking to do business with the Company, other than items of nominal value. Any gifts that are not of nominal value should be returned immediately and reported to your supervisor. If immediate return is not practical, they should be given to the Company for charitable disposition or such other disposition as the Company believes appropriate in its sole discretion. For the purposes of this Code, a gift of nominal value has a retail value of no more than $50.00.

Common sense and moderation should prevail in business entertainment engaged in on behalf of the Company. Employees, officers and directors should provide, or accept, business entertainment to or from anyone doing business with the Company only if the entertainment is infrequent, modest and intended to serve legitimate business goals.

Bribes and kickbacks are criminal acts, strictly prohibited by law. You must not offer, give, solicit or receive any form of bribe or kickback anywhere in the world.

Accuracy of Books, Records and Public Reports

Employees, officers and directors must honestly and accurately report all business transactions. You are responsible for the accuracy of your records and reports. Accurate information is essential to the Company's ability to meet legal and regulatory obligations.

All Company books, records and accounts shall be maintained in accordance with all applicable regulations and standards, and accurately reflect the true nature of the transactions they record. The financial statements of the Company shall conform to generally accepted accounting rules and the Company's accounting policies. No undisclosed or unrecorded account or fund shall be established for any purpose. No false or misleading entries shall be made in the Company's books or records for any reason, and no disbursement of corporate funds or other corporate property shall be made without adequate supporting documentation.

It is the policy of the Company to provide full, fair, accurate, timely and understandable disclosure in reports and documents filed with, or submitted to, the Securities and Exchange Commission and in other public communications.

Concerns Regarding Accounting or Auditing Matters; Prohibition against Retaliation

Employees with concerns regarding questionable accounting or auditing matters or complaints regarding accounting, internal accounting controls or auditing matters may confidentially, and anonymously if they wish, submit such concerns or complaints in writing to Dick Saporito in the Company's Human Resources Department or the Chief Financial Officer. In addition, you may file an anonymous complaint at http://www.MySafeWorkplace.com. All such concerns and complaints will be forwarded to the Audit Committee of the Board of Directors, unless they are determined to be without merit by the Human Resources Department and Chief Financial Officer of the Company. In any event, a complete record of all complaints will be provided to the Audit Committee each fiscal quarter. Any such concerns or complaints may also be communicated, confidentially and, if you desire, anonymously, directly to any member of the Audit Committee of the Board of Directors.

The Audit Committee will evaluate the merits of any concerns or complaints received, and will authorize such follow-up actions, if any, as it deems necessary or appropriate to address the substance of the concern or complaint. The Company will establish a toll-free telephone number where you may leave a confidential or anonymous message for the Audit Committee. The telephone number will be posted on the Company's Worknet website.

The Company will not discipline, discriminate against or retaliate against any employee who reports a complaint or concern (unless the employee is found to have knowingly and willfully made a false report).

Waivers of the Code of Business Conduct and Ethics

While some of the policies contained in this Code must be strictly adhered to and no exceptions can be allowed, in other cases exceptions may be possible. Any employee or officer who believes that an exception to any of these policies is appropriate in his or her case should first contact his or her immediate supervisor. If the supervisor agrees that an exception is appropriate, the approval of the Company's Human Resources Department and Chief Financial Officer must be obtained. The Human Resources Department shall be responsible for maintaining a complete record of all requests for exceptions to any of these policies and the disposition of such requests.

Any executive officer or director who seeks an exception to any of these policies should contact the CEO. Any waiver of this Code for executive officers or directors or any change to this Code that applies to executive officers or directors may be made only by the Board of Directors of the Company and will be disclosed as required by law or listing regulation.

Reporting and Compliance Procedures

Every employee, officer and director has the responsibility to ask questions, seek guidance, report suspected violations and express concerns regarding compliance with this Code. Any employee, officer or director who knows or believes that any other employee or representative of the Company has engaged or is engaging in Company-related conduct that violates applicable law or this Code should report such information to Dick Saporito in the Human Resources Department.

You may report such conduct openly or anonymously at http://www.MySafeWorkplace.com without fear of retaliation. The Company will not discipline, discriminate against or retaliate against any employee who reports such conduct in good faith, whether or not such information is ultimately proven to be correct, or who cooperates in any investigation or inquiry regarding such conduct. Any supervisor who receives a report of a violation of this Code must immediately inform Dick Saporito in the Human Resources Department.

You may report violations of this Code, on a confidential or anonymous basis, by contacting the Company's Human Resources Department by fax, mail or e-mail. The Company will establish a toll-free telephone number where you may leave a recorded message about any violation or suspected violation of this Code. While we prefer that you identify yourself when reporting violations so that we may follow up with you as necessary for additional information, you may leave messages anonymously. The telephone number will be posted on the Company's Worknet website.

If the Human Resources Department receives information regarding an alleged violation of this Code, he or she shall, as appropriate, (a) evaluate such information, (b) inform the Chief Executive Officer and Board of Directors if the alleged violation involves an executive officer or a director, (c) determine whether it is necessary to conduct an informal inquiry or a formal investigation and, if so, initiate such inquiry or investigation, and (d) report the results of any such inquiry or investigation, together with a recommendation as to disposition of the matter, to the Chief Executive Officer for action, or if the alleged violation involves an executive officer or a director, report the results of any such inquiry or investigation to the Board of Directors or a committee thereof. Employees, officers and directors are expected to cooperate fully with any inquiry or investigation by the Company regarding an alleged violation of this Code. Failure to cooperate with any such inquiry or investigation may result in disciplinary action, up to and including discharge.

The Company shall determine whether violations of this Code have occurred, and if so, shall determine the disciplinary measures to be taken. In the event that the alleged violation involves an executive officer or a director, the Chief Executive Officer and the Board of Directors, respectively, shall determine whether a violation of this Code has occurred and, if so, shall determine the disciplinary measures to be taken against such executive officer or director.

Failure to comply with the standards outlined in this Code will result in disciplinary action including, but not limited to, reprimands, warnings, probation or suspension without pay, demotions, reductions in salary, discharge and restitution. Certain violations of this Code may require the Company to refer the matter to the appropriate governmental or regulatory authorities for investigation or prosecution. Moreover, any supervisor who directs or approves of any conduct in violation of this Code, or who has knowledge of such conduct and does not immediately report it, also will be subject to disciplinary action, up to and including discharge.

Dissemination and Amendment

This Code shall be distributed to each new employee, officer and director of the Company upon commencement of his or her employment or other relationship with the Company. It shall also be distributed annually to each employee, officer and director of the Company. Each employee, officer and director shall certify below that he or she has received, read and understands the Code and has complied with its terms.

The Company reserves the right to amend, alter or terminate this Code at any time for any reason. The most current version of this Code can be found on the Company's Worknet website.

This document is not an employment contract between the Company and any of its employees, officers or directors and does not alter the Company's at-will employment policy.

Credit Card Processing Policy

Each employee has the responsibility to protect against the misuse of customer cardholder information provided to PC Connection; and to comply with all credit card industry regulatory requirements for collecting, processing, storing, or transferring cardholder information. PC Connection has established a commitment to protect the privacy and the security of all customer information provided through its various business activities. This commitment is established in the acceptable practices as outlined in this policy.

The PC Connection credit card program is managed in accordance with the Payment Card Industry (PCI) Data Security Standard. The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard customer information.[1] Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data.

Cardholder information is any information that can personally identify an individual to his/her account. This includes the account number, CVV2/CVC2/CID, expiration date of the account, address, telephone number, etc. Employees must protect the confidentiality of the card holder information at all times and not engage in practices that place the information at additional risk.

Authorization

The Chief Financial Officer (CFO) will set the standards of: retention, training, need-to-know, and establish who is authorized to engage in business processes involving card holder information. Business units wishing to engage credit card transactions or process card holder information are required to obtain the CFO's written authorization.

Communication

The credit card processing policy will be provided to all individuals at the beginning of their employment with PC Connection. The Policy will be made available on the corporate internal web site and distributed to all employees at a minimum of once each calendar year.

Procedures and Systems

All card holder processing procedures and electronic systems that process card holder data will be reviewed by the PC Connection PCI program manager. The PCI program manager working with assigned business unit managers will ensure that all card holder business processes and electronic processing systems are in compliance with PC Connection's privacy, security and regulatory requirements.

Processing

All transactions must be performed in accordance with approved procedures and on systems that are specifically approved for the processing of card holder information. Personnel are not authorized for, and are strictly prohibited from:

- Modifying any approved process that controls card holder information.
- Collecting, copying or storing card holder information in hard copy or electronic format except as part of an approved business processes.

- Transmitting any card holder information over unapproved systems. This specifically prohibits the transmitting of card holder information using Email.
- Email may be used, however, to transmit only redacted card holder information that contains only the name of the card holder and the last four digits of the account number.
- Divulging cardholder information to individuals who do not have an approved need-to-know.
- Attempting or attaining unauthorized access to any system or process that controls card holder information.
- Destroying or disposing of card holder information except as part of an approved business process.

[1] https://www.pcisecuritystandards.org/security_standards/index.php

Retention

Card holder information must only be retained as part of an approved business process and for only as long as there is a valid business need to retain the data as specifically authorized by the CFO.

Segregation of Duties

Credit card processing activities will be segregated to a sufficient level as to prevent unauthorized credit card processing, processing of refunds, and reconciliations of credit card transactions. The roles associated with the electronic processing of card holder data will be segregated so that a single individual or work center does not have complete control over the processing, maintenance, or storage of card holder data.

Technology Changes

All technology changes to systems that process card holder information must be authorized by the Chief Information Officer (CIO). Such approved changes must be performed using only approved change procedures.

Training

All personnel who conduct credit card transactions, process card holder data, or maintain electronic systems that control card holder data will be provided appropriate security training on acceptable credit card processing practices.

MOBILE DEVICE MANAGEMENT

PC Connection, Inc. and Affiliates

As an employee of PC Connection, Inc. family of companies, you may be permitted to access company data from a mobile device. This includes, but is not limited to; laptops, tablets and smartphones.

As set forth in the company's electronic communications policy, approved devices will contain software to remotely monitor the use of the device at any time. This functionality exists to protect company assets. In the event that a device is lost or stolen, the company has the ability to geographically locate and remotely lock or erase the device. As such, there is no expectation of privacy when utilizing company resources. Each employee, by accessing company data, expressly represents that they understand the policy and consent to such monitoring.

Company information available through the use of mobile devices is proprietary and for company business only. Such information may be confidential and may not be used or disclosed, except as approved by management. Improper access or use of the mobile device or improper disclosure of confidential information may result in disciplinary action up to and including termination.