

**PUSTORINO, PUGLISI & CO., LLP  
(PP&CO)  
FIRM POLICIES ON PROTECTION OF  
PERSONAL IDENTIFIABLE INFORMATION**

## **I: Personal Identifiable Information (“PII”)**

Confidential information is any non-public information that comes to a PP&CO personnel’s (employee, partner, contractor/consultant) attention as a result of the personnel’s association with PP&CO or Firm. This nonpublic information may relate to current clients, former clients or nonclients and may include PII.

PII is a type of confidential information and generally refers to information that (a) is about, or pertains to, a specific individual (client or otherwise), (b) can be linked to that individual, and (c) can be used to identify that individual. Information that pertains to a specific individual, but that can not be used to identify that individual, is not considered to be PII.

PII may include, but is not limited to, name, address, phone number, e-mail addresses, financial and bank account numbers, social security numbers, medical information, photos, static IP addresses, and date of birth.

Specific PII areas for PP&CO are indentified below.

## **II: Responsibility**

PP&CO personnel are to exercise due care and comply with all applicable professional standards in determining whether information is confidential and in maintaining confidentiality and privacy.

Confidential information relating to the collection, access, use, distribution and protection of PII complies with client agreements, professional standards, personal information laws and regulations.

PP&CO personnel are to treat PII in a way that respects the privacy of individuals in the fair processing of PII.

PP&CO personnel are not to discuss confidential information, including PII, with individuals, including individuals inside the Firm, who do not have a business need to know the information. Disclosures authorized by the client or where there is a professional or legal duty to disclose are permitted. Additionally, consultations with appropriate PP&CO persons on technical, ethical or other issues are permitted provided that reasonable care is taken to ensure that those consulted are aware of the confidential nature of the information and reasonable efforts are made to confirm that there are no conflicts of interest prior to the consultation.

Unless there’s a business need to know the information, PP&CO personnel are not to seek out confidential information, including PII. Nor are they to discuss confidential information in a public place or a social environment. Where client engagement matters are discussed, heightened awareness and appropriate care are to be exercised to protect confidential information from unauthorized disclosure.

### **III: Confidentiality Requirements**

- Rule 301 of the AICPA Code of Professional Conduct states:  
“A Member in public practice shall not disclose any confidential client information without the specific consent of the client”

**Firm personnel are required to maintain confidentiality of client and former client information, as well as information of nonclients that is known to be confidential. Nonclient information, as it pertains to PP&CO, is generally obtained through proposal opportunities and the rendering of due diligence services.**

**Particular care is also required to maintain confidentiality of client information that is on a computer, contained in e-mail or otherwise conveyed on the internet.**

**The Firm restricts access to, and maintains control over, its working papers. Working papers are only made available to clients or others outside PP&CO only with prior approval of the engagement partner.**

### **IV: Confidentiality Affirmation**

**Firm personnel are required to affirm their understanding of the treatment of confidential client information in writing upon commencement of employment and annual thereafter. Additionally, professional personnel are required to affirm their understanding of the AICPA rules governing confidential information and independence requirements each calendar year.**

**Violations of firm policy or law, including those related to privacy and the protection of PII should be reported to the managing partner or to any other partner. Such violations may result in discipline, up to and including termination.**

### **V: Training**

**All Firm personnel must become familiar with these rules and each one is responsible for abiding by it. The partners and managers of the Firm will enforce the policy and be available to answer any questions relating to it. The input and recommendations of all personnel is welcomed and encouraged.**

### **VI: Occurrence**

**In the event of a PII theft occurrence, PP&CO will notify the affected person(s) and work with them as well as credit bureaus and law enforcement people to protect people from, or minimize any potential damage, that the theft may cause.**

## IDENTIFIED AREAS

The following are areas that where PII is located for PP&CO. These areas are not meant to be all inclusive and there may be other instances of where PII is applicable and, as such instances become available, they will be added to this list. Additionally, this document, in and of itself, is PII and subject to all the Firm policies mentioned above.

1. Staff lap top computers used in the field.
2. Data stored on home computers.
3. Data transported back and forth through the use of USB and other similar devices.
4. Paper files in the office (tax information, audit and accounting files, etc.).
5. Data stored at Globe Storage and Moving.
6. Blackberries and other similar devices used to access office servers.
7. Mail and faxes received and not distributed to recipient.
8. E-mail attachments.

## SECURITY PROCEDURES

1. All laptops are password protected and the access to our server requires an additional password. All laptops are to be in the possession of the staff member at all times and are not to be left at the client's office unless they are stored in a locked facility with only PP&CO personnel having the key. In the event of a loss or theft, you must notify a partner immediately. As for data stored on the laptop hard drive, it is to be deleted upon transferring to the office server. PII is to be kept to a minimum on laptops, i.e., when performing work that requires the use of data that is personal in nature (SS #, bank account #, etc.), this data is to be expunged and, if possible, not recorded on the work paper. For example; when doing work on payroll data for a client, there's no need to record the SS# of an employee, in that case, you should assign a random # to identify the person and make appropriate comments that the SS# was used but not recorded.
2. There will be no data stored on home desktop or personal laptop computers that contain any PII on clients of the Firm or any Firm PII.
3. The use of USB storage or similar devices should be kept to a minimum and, when used, the device has to be password protected. As in procedure #1 above pertaining to laptops, the same procedures apply to these devices.
4. Effective November 1, 2009 the Firm will institute a "Clean Desk Policy". This will require that every Firm personnel clean his/her desk each and every day of any PII; there's to be NO files left on a desk that contain any PII. All PII has to be placed in drawers and file cabinets and locked. During the day an effort has to be made to keep any unattended surface free of PII.

Information such as bank statements, 1099s, brokerage statements, etc. should be scanned and placed in a PDF format on the server. Where scanning is not practical, the practice of locking up the data should be followed. Data that we have no use for after the completion of the tax return, audit or other service, if original, should be sent back to the client; copies must be shredded.

5. **Globe Storage and Moving Co., Inc. stores our files and keeps an inventory of all our boxes. Globe has security policies whereby its warehouses have alarms, video surveillance and require that access to any data be pre-approved and any one visiting the facility to retrieve data is accompanied by a Globe employee and is properly identified. Globe also requires pre-approval from any of its customers before data is removed and/or accessed. PP&CO reviews its storage inventory on a regular basis and removes and destroys data that is past our retention policies (anywhere from 7-10 years depending on the data).**
6. **Blackberry and other similar devices that enable an employee to access the Firm Exchange server, must be password protected and must not be left unattended at any time. In the event of a loss or theft of the device, please notify one of the partners immediately.**
7. **Every effort will be made to distribute the daily mail. When it cannot be accomplished, the mail person (generally the receptionist) will hold on to the mail until the recipient is available to receive it. Depending on the content, the undistributed mail will be kept by the receptionist in a secure location. Mail that is considered not to be confidential will be placed on the recipient's desk. The recipient can also instruct the receptionist on where to store the mail while he/she is away. Faxes should be similarly handled; under no circumstances should any fax containing PII be placed on the desk of the recipient if that person is out of the office. The Firm's new phone system will have the capability to direct any faxes directly to the recipient's e-mail address. It is each person's responsibility to ensure the security of incoming faxes that contain PII.**
8. **Any e-mail attachment must be secured similarly to any other electronic data containing PII and must be transferred directly to the client's file on the Firm server. Outgoing email attachments containing PII should be placed in a Zip file and must be password protected. Our new Portal program will add further protection to information exchanged through e-mails.**