AICPA® Privacy

This checklist provides CPA firms with practical illustrations of selected Generally Accepted Privacy Principles (GAPP) in order to maintain privacy best practices within their organizations. Not all recommendations will apply to all firms.

A Privacy Checklist FOR CPA FIRMS

1 Notice – The firm provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.

CPA FIRM PRIVACY STATEMENT

Although CPA firms are no longer subject to the notice requirements of GLBA, the AICPA's Generally Accepted Privacy Principles (GAPP) and good business practice recommends that the CPA publish their Privacy Statement. The privacy statement may use the standard statements required by GLBA.

2 Security for Privacy – The firm protects personal information against unauthorized access (both physical and logical).

EMPLOYEE INFORMATION

As an employer, you have personal information about your employees such as:

- Social Security Number
- Bank Account Information
- Medical Information
- Benefit Information

This information should be kept secure and restricted to only those individuals with a business reason to have access.

CLIENT TAX INFORMATION

Clients' tax returns containing personal information should be secured and restricted to only those individuals with a business reason to have such access. In order to prevent unauthorized access to tax return information, it is good business practice to password-protect all electronic files containing this information.

For tax return documentation maintained in hard copy, these files should be kept secured and in a location where visitors do not have access.

TRANSMITTING CLIENT DATA

When transmitting client data by e-mail using the Internet, the e-mail and/or attachments containing client personal information should be encrypted and password protected. A common password system is the use of the last 4 digits of the taxpayer's Social Security Number. Using this method insures that the recipient must already know the taxpayer's Social Security Number in advance.

If the information is sent via facsimile, verify with the intended recipient that the fax number is correct and the fax machine is in a secure location. A cover sheet should be used with the appropriate disclosures regarding IRS Circular 230.

When sending by mail, the documents should be sent either by certified mail or by a carrier that will require a signature from the receiving party.

CONTINUED >

COMPUTER SECURITY

All computers should be password protected. Each user should sign-in with a unique ID and password. Passwords should be a minimum of eight characters made up of numbers, letters and characters. Passwords should be changed on a regular basis and at least every 60 days. Laptop files containing personal client or employee information should be encrypted, and protected with passwords similar in complexity to those used to secure the computer device on which they reside. Some hard drive manufacturers are now manufacturing hard drives that feature built in encryption.

SERVERS

In addition to their regular user ID, Server Administrator(s) should have a separate and unique administrative ID and password for use only when performing system administration activities. System default IDs and passwords should be changed immediately. The administrative password should be longer than the regular user passwords, with a minimum of 12 digits.

COMPUTERS CONNECTED TO INTERNET

Various security practices should be utilized for computers connected to the Internet. These practices include firewalls, up-to-date anti-virus software, current software security patches and spyware.

WIRELESS TRANSMISSIONS

Many firms have a wireless access point in their offices, either for their use or their clients. When installing the access point, it should be password-protected so that someone close by can not log into the network and access the firm data. If the office already has a hard-wired network, then if possible, the access point should be outside the network so no-one can hack into the servers.

REMOTE ACCESS

Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access client data at home. Also, require employees who use personal computers to store or access client data to use protections against viruses, spyware and other unauthorized intrusions.

CREDIT CARD INFORMATION

Many firms have their clients' credit cards numbers on file. This information should be kept secure to prevent unauthorized access and should not be retained longer than needed.

COMPUTER BACKUPS

Computer backups containing personal information should be kept secure and, if appropriate, encrypted. A copy of the backup also should be kept in a secure off-site location.

3 Management – The firm defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

EMPLOYEE TRAINING

All employees should be educated on the importance of keeping Personal Information secure in and out of the office.

4 Disclosure to Third Parties – The firm discloses personal information to third parties only for the purposes identified in the notice and with implicit or explicit consent of the individual.

Personal Information about your clients is disclosed to third parties only for purposes described in the notice and for which the client has provided implicit or explicit consent.

5 Use and Retention – The firm limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The firm retains personal information for only as long as necessary to fulfill the stated purposes.

FILE RETENTION/DESTRUCTION POLICY

All firms should establish a policy on how long to retain client information. At the end of the retention period, the information should be either returned to the client or properly destroyed. For paper information, it should be shredded. For electronic data, ensure client information is deleted and written over to make it unrecoverable.

For additional information on GAPP and its principles, criteria, and illustrations that CPA firms should consider, refer to ***www.aicpa.org/privacy****.*

AICPA®