

Protecting Client Data: Is My Firm At Risk?

Does your firm maintain sensitive personal data* (e.g., social security numbers, financial data, etc.) for clients?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If the sensitive personal data is maintained in paper format, such as audit papers or tax returns, do you allow employees to take this information out of your office?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Is any of the sensitive personal data maintained in electronic format?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Does your firm maintain sensitive personal data on file servers that are connected to the Internet?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do staff members copy sensitive personal data to laptop hard drives or memory sticks that are allowed to leave the office?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do you have an e-mail system that allows anyone in your firm to transfer any document stored on your internal network to anyone outside your firm?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do you allow wireless connections to your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Does your firm allow employees to access network resources using remote access technologies or a virtual private network (VPN)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do you send client data files to outsourcing companies?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do your employees allow vendors to provide technical support by remotely connecting to your firm's computers?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Are your employees allowed to send client data files to your vendor's technical support representatives using unsecured e-mail?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

If you answered "Yes" to any or all of these questions, your firm is a risk of exposing your clients' sensitive personal data. This exposure may cost your firm a significant amount of money and permanently tarnish your firm's reputation. The following is a series of questions that will help assess if you have implemented policies and procedures that will protect your clients' data.

* As defined by the AICPA Generally Accepted Privacy Principles (GAPP) – see <http://www.aicpa.org/privacy>

Mitigating Your Risk

Does your office have an alarm system?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Are your network servers located in a restricted area?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Are you using a firewall to protect your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Does your firm have a Data Protection Policy?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do you require strong passwords to access network resources?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do you use two-factor authentication on your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Are you using encryption technology to protect the information stored on your laptop hard drives and memory sticks?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do you use locking cables to secure your laptop computers?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Does your firm use secured email or a client portal to securely exchange data files with clients?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Is your firm familiar with your responsibilities under California Senate Bill 1386 or the 31 other state security breach notification laws?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Has your firm developed an incident response plan that would be followed in case of the loss of sensitive client data?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Does your firm use any technology to track a stolen laptop?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Have you installed software that can remotely erase a laptop hard drive in case it is lost or stolen?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Do your employees receive training with regard to the firm's data protection policies and procedures?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

© 2007, American Institute of Certified Public Accountants, Inc.

This checklist is part of a series of Content Suites created by the AICPA's IT Executive Committee to help Information Technology Section members and Certified Information Technology Professional (CITP) credential holders in their everyday technology life. For more information on the AICPA's technology initiatives, including its Content Suites, the CITP Credential and the IT Membership Section, visit <http://www.aicpa.org/infotech>. Additional information on data protection, including privacy management, may be found at <http://www.aicpa.org/privacy>. Any hardware or software products mentioned do not in any way represent an endorsement by the Institute or Section.