



**CLIENT MEMO**  
**COMPUTER DOCUMENT AND INTERNET SECURITY**  
**(January 2012)**

As computer and internet become vital to every organization, it is important to adopt security policies to safeguard and manage these company resources. We have listed a few security policy recommendations as follows:

1. **Passwords** to limit workstation and confidential information access to authorized personnel only. Passwords should be kept secured, changed at regular intervals (preferably every 90 days), and promptly canceled for terminated employees. Whenever possible, you should set up separate passwords for each individual program, separate and apart from the system password. There should also be a policy to confirm that all terminated employees are denied access to company computer systems both internally and through remote connections (i.e. Citrix or Remote Desktop). It is helpful to have a list of what every employee has access to, including not only the internal computer resources, but also any external vendor websites that employees may have separate user accounts for.
  
2. **Daily backup and disaster recovery plans** should cover procedures for daily back-up and off-site and onsite storage of programs and data files. Additionally, off-site storage for master files and copies of all software programs and licenses should be established to enable recreation of the current master files and system documentation in the event of a disaster. There should be written documentation containing instructions for starting and logging into all servers, with the passwords and instructions to reboot any server including from remote locations. These instructions should be kept confidential. These plans should also provide for alternative processing in the event of loss or interruption of service. Test restores and alternative processing should be performed and documented at least monthly. Technology has progressed to the point where tape backup is no longer the most effective and efficient method of backup. Use of Disk Based and Online Backup (DBOB) systems enables you to take snapshots of your data and programs, over an encrypted connection, and send the backup to one or more collocation facilities out of state. We highly recommend that these “cloud-based” systems be researched and we can make a recommendation and referral to a vendor whom we have a high degree of confidence in if you need assistance.
  
3. **Firewalls** are effective filtering devices designed to permit or deny access to communications via the internet. Not only can firewalls prevent users from illegitimately downloading malicious software to the network, they can also eliminate unauthorized personal use of company equipment by blocking access to non-business related websites (i.e. pornography, social networking, shopping, and gambling). However, if you have a firewall that is older than 3 years, it is advisable to replace or update it.



4. **Internet redundancy** – We recommend having dual sources of internet connections (i.e. DSL or T-1 and Cable) to provide for uninterrupted internet connection in the event of an outage. This can be done in a cost effective manner, and be configured through dual firewalls and routers to provide for automatic switch over.
  
5. **Hardware security** –
  - Servers should be maintained in a locked rack located in a locked room with proper independent cooling systems.
  - Each workstation, server, phone and voice mail systems should be protected by a power surge protector or small battery backup unit, and auto shut-down software.
  - Voice mail systems can be backed up along with the data systems.
  - CPUs should be lifted off the floor on a stand to reduce the amount of dust build up inside the case which would compromise the processing efficiency of the unit.
  - Workstations should lock automatically after a period of inactivity and should be logged off each night. Password should be required to regain access.
  
6. **A blanket fidelity bond** should be obtained to cover all MIS personnel. A policy to provide for reimbursement for data loss and recovery should also be obtained. This policy should include coverage for loss of valuable paper documents.
  
7. **Document management** – We believe strongly in replacing traditional paper-based files with paperless document management systems. We have been paperless for almost ten years without any paper files or folders. This practice, in our view, offers the best protection against fire, theft, and loss, and provides tremendous efficiencies and the ability to access any files from anywhere with an internet connection. In addition, the flexibility to make certain files available to certain staff member is unparalleled. We can make a recommendation to a vendor if you have an interest.

One key to create effective security policies is to first create a culture of security. By making it clear to employees the security concerns over computer document and internet access enhances cooperation and compliance with implementation of the security policies.

We encourage you to review the above suggestions and contact us for assistance to assessing your particular security needs. You may view a copy of this and other FBD memos on our website under PUBLICATIONS/Client memos - <http://www.fbco.com/publications/Client memos>.

**FISHMAN, BLOCK + DIAMOND, LLP**

16830 Ventura Boulevard, Suite 400  
Encino, California 91436  
Tel 818.783.7140 310.284.8267  
Fax 818.783.3706  
Web [www.fbco.com](http://www.fbco.com)