



7 STEPS TO SECURE DIGITAL FILES

1. **Lock up sensitive paper files.**
2. **Use enterprise-grade Wi-Fi in your office.**
3. **Ban public use of company devices.**
4. **Install antivirus, anti-spyware and firewalls.**
5. **Regularly update all systems and software.**
6. **Evaluate contractor access to information.**
7. **Properly dispose of technology tools.**

Brought to you by:



BREACH PROTECTION TIPS FOLLOW THESE STEPS TO SECURE DIGITAL FILES

Limit the use of portable technology.

Limit the use of portable technology. Restrict the “Bring Your Own Device” (BYOD) trend to the most secure devices. To reduce risks, don’t store non-confidential data on these devices. If your IT policy allows confidential information to be shared on BYOD devices, make sure the information that’s transferred and stored is encrypted and password-protected.

Use enterprise-grade Wi-Fi in your office.

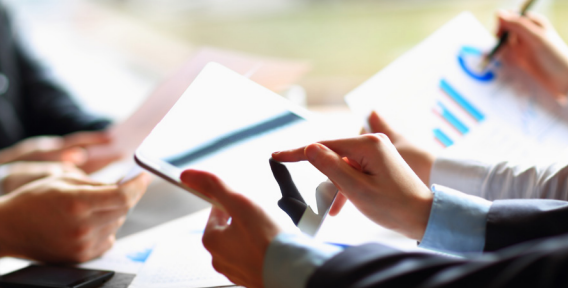
It must be secure, encrypted and behind a firewall. Access should require a unique username and password centrally controlled through the Wi-Fi hardware or an external directory authentication service. Integrating Wi-Fi with a directory service such as Microsoft Active Directory provides improved security. That’s because the credentials provided are the same as the standard network logon credentials. They must follow the same complexity and rotation rules.

Ban public use of company devices.

Public Wi-Fi hotspots such as those in hotel lobbies, coffee shops or airports can put your laptop or device in a network that can give hackers and thieves access to your data. Wireless and hard-wired connections in hotel rooms should not be trusted to access company email and servers. Instead require employees to use a company-provided wireless broadband card to ensure data security.

Install antivirus, anti-spyware and firewalls.

Help prevent the mining of sensitive information by worms, Trojan horses, viruses and more, by installing the most recent enterprise-level antivirus, anti-spyware and anti-malware applications. Use firewalls to lock out hackers. »



Regularly update all systems and software.

Keep protection up-to-date by downloading recently issued system “patches” from antivirus and anti-malware registries, to defend against the latest forms of viruses, Trojan horses and other malicious software.

Evaluate contractor access to information.

Evaluate whether contractors and vendors need access to any sensitive data. For example, employee personally identifiable information should only be accessed for payroll or benefit purposes.

Your vendor agreements should provide adequate safeguards and ask vendors to: (a) abide by reasonable industry safeguards, (b) cover the costs and handling of any misuse or loss of sensitive data by their employees, and (c) have the financial capability to cover the costs to restore loss or damage, including remediation, by insurance coverage or bond.

Properly dispose of technology tools.

Establish policies on how to destroy old computers, disks, tapes, CDs, memory devices and any other equipment that may contain sensitive information to prevent access by thieves. Don't rely on the delete or trash functions to remove confidential files. To ensure complete destruction of the files, destroy the device.

Brought to you by:

