COUNTRY FINANCIAL®

AUTO | HOME | LIFE | BUSINESS | RETIREMENT

Dealing with Technology

PROTECTION TIPS FOR YOUR BUSINESS DATA

- **Limit the use of portable technology.**
  Restrict the transfer of sensitive information from on-premises computers to portable devices such as cell phones, PDAs, laptops, USB flash drives and removable hard drives. If it is necessary to put confidential data on these devices, make sure information is encrypted and password protected.

- **Don't use wireless networks.**
  Even when properly secured, off-the-shelf wireless networks do not provide adequate enterprise level security to safeguard confidential data. As a standard rule, refrain from using wireless networking technology (Wi-Fi) to access systems storing sensitive personal information.

- **Utilize password protection and encryption.**
  Always encrypt sensitive information. Inexpensive or even free encryption technologies are readily available. All system users should be assigned unique user names and passwords, changed quarterly.

- **Install antivirus, anti-spyware and firewalls.**
  To prevent the loss or mining of sensitive information by worms, Trojan Horses, viruses, etc., run all systems with the most recent enterprise level antivirus, anti-spyware, and anti-malware applications. Use firewalls to lock out hackers.

- **Regularly update all systems and software.**
  To maintain the most up-to-date protection, download recently issued system "patches," antivirus and anti-malware registries containing the newest forms of viruses, Trojans Horses and other malicious software.

- **Evaluate contractor access to information.**
  Review and consider any and all access that outside contractors or vendors have to sensitive data and determine the need for such access. For example, access to employee personally identifiable information should only be for payroll or benefit purposes. Be sure that relevant vendor agreements provide adequate safeguards and that vendors agree to: (a) abide by reasonable industry safeguards; (b) cover the costs and handling of any misuse or loss of sensitive data; and (c) have the financial capability, whether through a bond or insurance coverage, to pay for any required remediation in the case of a loss of information.

- **Properly dispose of technology tools.**
  Implement policies on how to destroy old computers, disks, tapes, CDs, memory devices and any other equipment that may contain sensitive information. Often these devices can provide access to sensitive information, even if the information is deleted. Do not rely on the "delete" or trash function to remove files containing sensitive information. It is often best to physically destroy the devices when they are no longer needed.

Brought to you by:

COUNTRY FINANCIAL®

AUTO | HOME | LIFE | BUSINESS | RETIREMENT

Powered by

IDT911

Protecting Identities. Enhancing Reputations.