COUNTRY FINANCIAL®

AUTO | HOME | LIFE | BUSINESS | RETIREMENT

Taking Care of the Basics

PROTECTION TIPS FOR YOUR BUSINESS DATA

- **Lock up sensitive data.**
  File storage such as cabinets, file rooms or other areas that store files containing private data about customers, clients, patients, accounts, employees, etc., should be locked.

- **Restrict access to data.**
  Sensitive information, whether physical or electronic, should only be accessible to those who have a "need to know." Put written procedures in place defining who has access to restricted information. Set up computer networks that only permit designated people to have access to specific areas or files on the computer network. Remember to limit network access on computer stations located in public spaces like the reception area. Most employees do not need unfettered access to the entire company network.

- **Determine what information is necessary.**
  Don't collect and keep data that is not absolutely necessary. Collecting excessive personal information, like Social Security numbers, can be more of a liability than an asset. What's more, storing sensitive information longer than necessary or legally required exposes companies to unwanted risks. Put a retention policy in place and be sure to destroy outdated information in a secure manner.

- **Put security systems in place.**
  Install an alarm system that alerts law enforcement if you have a break-in on your premises. If feasible install video surveillance equipment and motion sensitive cameras on premises to monitor activities. In addition, random or roving security patrols add an extra layer of security.

- **Require sign-in for non-employee visitors.**
  Prior to being allowed on company premises, all visitors should have to show identification and sign in. This includes vendors, policyholders and prospective employees. Severely restrict or prohibit visitor access to areas containing files or other sensitive information.

- **Screen all employees.**
  Implement hiring practices for all employees, especially those with access to sensitive information. Use criminal and background screening companies. All employees who have access to sensitive information—including cleaning crews, technicians, administrative assistants, temporary employees—should sign a confidentiality and security document.

- **Define and regularly review data practices.**
  Distribute and explain data protection protocols to all employees. Review and revise these practices on a regular basis, at least once a year. Retrain staff when protocol changes are made.

- **Review security procedures.**
  Put best practice policies in place and evaluate them on a regular basis. Make sure: (a) sensitive files are locked up when not in use; (b) only authorized users can access confidential information; (c) sign-in logs are maintained; and (d) documents and data are properly destroyed.

Brought to you by:

COUNTRY FINANCIAL®

AUTO | HOME | LIFE | BUSINESS | RETIREMENT

Powered by

IDT911

Protecting Identities. Enhancing Reputations.