Keeping Insider Information Inside

What is a company's most valuable property? It isn't buildings or equipment, but information - from computer files and training materials to budgets and product research.

When vital "insider" information leaves the organization improperly, everyone loses. Profits can drop, reputations can be damaged, employees can lose jobs, and morale can plummet.

"Inside" or Confidential Information Includes:

- *Organizational information* - telephone directories, organizational charts, training materials, personnel files and policies, salary scales, performance evaluations, telephone and computer codes.
- *Financial* - budget reports, sales and order volumes prior to public release, production and overhead costs, profit margins, payroll procedures.
- *Marketing* - short and long-term strategies, customer lists, market research results.
- *Research and Development* - technical and performance specifications, reports on research in progress, project code names, blueprints, test and system software.
- *Manufacturing and Production* - vendor names, production levels, inventories, future plans and sites, product failure reports.

Put a lock on your company's information!

- Think before talking about the details of your job in public places such as restaurants, airplanes, classrooms, gyms, and parties.
- Know who's on the other end of the line -telephone, modem, or fax- before giving out any sensitive information. It could be a competitor or trade journalist looking for helpful employees who are too eager to give out information about their employer.
- Keep your work area clear. When you will be gone for a few hours, or at the end of the day, put sensitive papers in a drawer or file cabinet.
- Think about what's on a piece of paper before you toss it into the trash. If it's sensitive information, tear it up or use a shredder.
- Challenge strangers who enter your work area unescorted. Call a supervisor or security for help.
- Protect identification badges, office keys, and codes as you would your own cards and keys.

What's in a password?

Most computer systems have complex built-in security devices, but the right password can still unlock the system! Make it hard for "information thieves" to figure out your password.

- Use at least eight characters. Avoid personal information like date of birth, address, or social security number.
- Add a punctuation mark or number if your system permits.
- Use a phrase instead of a one-word password if possible.
- You might choose a word in English, then use a dictionary to translate it into a foreign language.
- Change your password monthly.
- Memorize your password. Don't write it on a piece of paper inside your desk drawer, appointment book or on a rolodex.

Cracking the voice mail or PBX system.

Remote access and voice mail features of PBX (private branch exchange) systems make them vulnerable to con artists who specialize in toll card fraud. To stop these thieves from running up phone bills on your company's account:

- Change your access code frequently, and use longer codes.
- Treat you phone password like your computer password - with extreme care!
- When you're away from the office, don't let anyone see or overhear your phone card codes.

When you travel on business...

- Resist discussing your job with the friendly person next to you.
- Avoid the temptation to work on sensitive projects in public places like restaurants and planes.
- When you leave your car or hotel room, put company information in a secure place or take it with you.
- Be sensitive to conducting confidential business on the phone, including cellular phones.

A Final Note

When you were hired, you may have signed an agreement regarding the protection of proprietary information. This is a legally and ethically binding contract between you and the company. Take it seriously!