SECTION 3: SAFETY AT THE OFFICE

Safety at the Office

Apply the following safety procedures to help keep you and your belongings safe at the office:

General Security Measures

— Know staff in other nearby businesses and be aware of their schedules.

— Ensure all doors other than the main entrance are secured.

— Make certain windows are not obscured so that passersby can see in.

— Make sure there is a clear exit route from the service desk to the door.

— Never allow visitors to wander freely about the business. Have the person whom they want to see come to the front office area and escort the individual to the meeting area.

— Have a visitor log book and policy on issuing visitor tags that limit access to certain areas and hours of the day.

— If you encounter an individual while working late or alone, indicate to that person that you are not alone. Say something like, "My supervisor will be right with you and should be able to assist you."

— Keep personal information private. Avoid discussing where you live, after-work or vacation plans in front of customers, new coworkers or anyone with whom you are not comfortable.

— Install a spare phone in the storage room.

— Install an alarm, (preferably both audible and monitored). Have alarm buttons in strategic spots; i.e. panic buttons at the reception area.

— Install surveillance cameras that will monitor the front entrance, the reception area, and other areas that are accessible to the public.

CONTINUED

Personal Valuables and Equipment

— Never leave valuables, purses or wallets tucked behind counters or on desks.

— Lock away personal letterhead and business cards to avoid use by unauthorized people.

— Mark equipment for easy identification in the event of theft or damage. Maintain an inventory of all marked items.

— Lock up audio/visual equipment when not in use.

— Secure spare and master keys in locked cabinets.

Protect Client Information

Most offices keep sensitive personal information on their computers and/or in paper files—names, Social Security numbers, credit card or other account data—that identifies customers or employees. If this sensitive data falls into the wrong hands, it can lead to fraud or identity theft.

State and federal laws govern how personal information should be disposed of. Specifically, the Federal Trade Commission (FTC) has a Disposal Rule that requires businesses to adopt appropriate disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. Be sure you check for applicable laws that will dictate how you handle and dispose of personal information.

A sound data security plan is built on 5 key principles:

1. **Take stock.** Know what personal information you have in your files and on your computers. Effective data security starts with assessing what information you have and who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities.

CONTINUED

2. Scale down. Keep only what you need. If you don't have a legitimate business need for sensitive identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary. If only one or two employees need access to personal information, make sure access is limited to only those employees.

3. Lock it. Protect the information that you keep. The most effective data security plans include physical security, electronic security, employee training, and the security practices of contractors and service providers.

4. Pitch it. Properly dispose of what you no longer need to ensure that it cannot be read or reconstructed. Check your state laws regarding destruction of personal information to make sure you're in compliance.

5. Plan ahead. Create a plan to respond to security incidents. Have a plan in place to respond if there is a security breach. Designate a senior member of your staff to coordinate and implement the response plan.

Access to Your Office

— Restrict office keys to those who need them. Maintain a record of keys, including issue and return dates, name and signature of recipient and an outline of the consequences should an important key be missing.

— Mark office keys with "Do Not Duplicate."

— Establish a rule that keys are not to be hidden or left unguarded on desks or cabinets and enforce that rule.

— Have a procedure in place for collecting keys and IDs from terminated employees.

— Treat doors with coded locking systems as you would a key. Codes are released to appropriate individuals only, and should be changed as those individuals leave your employment. Have a procedure in place for the release of these codes.

(Sources: Sonoma County Crime Crushers; Federal Trade Commission)