DATA SECURITY BEST PRACTICES: 1 OF 5

1. Take Stock

- Inventory all file storage and electronic equipment.
- Ensure sensitive data is stored securely.
- Talk with your employees and outside service providers to determine who sends personal information to your business and how it is sent.
- Consider all the ways you collect business and employee personal information from customers, and what kind of information you collect.
- Review where you keep the information you collect and who has access to it.

CAP COM
Business Services

DATA SECURITY
BEST PRACTICES: 2 OF 5

2. Scale Down

- Use Social Secutiry numbers only for required and lawful purposes. Don't use SSNs as employee indentifiers or Company locators.
- Keep Company credit card information only if you have a business need for it.
- Review the forms you use to gather data - like credit applications and fill-in-the-blank web screens for potential customers and revise them to eliminate requests for information you don't need.
- Truncate the account information on electronically printed credit and debit card receipts you give your customers. You may include no more than the last five digits of the card number, and you must delete the card's expiration date.
- Develop a written records retention policy, especially if you must keep information for business reasons or to comply with the law.

CAP COM
Business Services

DATA SECURITY
BEST PRACTICES: 3 OF 5

3. Lock It

- Put documents and other materials containing personally identifiable information in a locked room or file cabinet.
- Remind employees to put files away, log out of computers and lock file cabinets and lock their offices at the end of the day.
- Implement appropriate access controls for your building.
- Encrypt sensitive information if you must send it over public networks.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers.
- Require employees to use strong passwords. Use eight or more characters witha combination of at least 1 upper case letter, 1 lower case letter, numbers and special characters. Change your password atleast every 6 months.
- Set "access controls" to allow only trusted employees with a legitimate business need to access the network.

CAP COM
Business Services

DATA SECURITY BEST PRACTICES: 4 OF 5

4. Pitch It

- Create and implement information disposal practices.
- Dispose of paper records by shredding them.
- Defeat dumpster divers by encouraging your staff to separate the stuff that's safe to trash from sensitive data that needs to be discarded with care.
- Make shredders available throughout the workplace including next to the photocopier.
- Use wipe utility programs when disposing of old computers and portable storage devices.

CAP COM
Business Services

DATA SECURITY BEST PRACTICES: 5 OF 5

5. Plan Ahead

- Create a plan to respond to security incidents, and designate a response team lead by a senior staff person.
- Draft contingency plans for how your business will respond to different kinds of security incidents.
- Investigate security incidents immediately.
- Create a list of who to notify, inside or outside your organization, in the event of a security breach.
- Immediately disconnect a compromised computer from the internet.

Sourced from the Federal Trade Commision: Protecting Personal Information: A Guide for Business

CAP COM
Business Services