Today, virtually all businesses collect and store personal information about customers, employees, and others. The frequency of data breaches — the theft, loss or mistaken release of private information — is on the rise. And it’s not just a big business problem. Small and mid-sized businesses with fewer data security resources are particularly vulnerable.

As a result, it’s important for business of every size to take steps to prevent a data breach. Here’s how:

1. **Keep Only What You Need.** Inventory the type and quantity of information in your files and on your computers. Reduce the volume of information you collect and retain only what is necessary. Don’t collect or keep information you don’t absolutely need. Minimize the number of places you store personal private data. Know what you keep and where you keep it.

2. **Safeguard Data.** Lock physical records containing private information in a secure location. Restrict access to that information to only those employees who must have access. Conduct employee background checks. Never give temporary workers or vendors access to personal information on employees or customers.

3. **Destroy Before Disposal.** Cross-cut shred paper files before disposing of private information. Also destroy CDs, DVDs and other portable media. Deleting files or reformatting hard drives does not erase data. Instead, use software designed to permanently wipe the hard drive, or physically destroy the drive itself. Also, be mindful of photocopy machines, as many of these scan a document before copying. Change the settings to clear data after each use.

4. **Update Procedures.** Do not use Social Security numbers as employee ID or client account numbers. If you do so, develop another ID system immediately.

5. **Educate/Train Employees.** Establish a written policy about privacy and data security and communicate it to all employees. Require employees to put away files, log off their computers and lock their offices/filing cabinets at the end of the day. Educate employees about what types of information are sensitive or confidential and what their responsibilities are to protect that data.
6. Control Computer Usage. Restrict employee usage of computers to business use. Don’t permit employees to use file sharing peer-to-peer websites or software applications, block access to inappropriate websites and prohibit use of unapproved software on company computers.

7. Secure All Computers. Implement password protection and ‘time-out’ functions (requires re-login after periods of inactivity) for all computers. Train employees to never leave laptops or PDAs unattended. Restrict telecommuting to company owned computers. Require the use of strong passwords that must be changed on a regular basis. Don’t store personal information on a computer connected to the Internet unless it is essential for conducting business.

8. Keep Security Software Up-To-Date. Keep security patches for your computers up-to-date. Use firewalls, anti-virus and anti-spyware software; update virus/spyware definitions daily. Check your software vendors’ websites for any updates concerning vulnerabilities and associated patches.

9. Stop Unencrypted Data Transmission. Mandate encryption of all data transmissions. This includes data ‘at rest’ and ‘in motion’. Also consider encrypting email within your company if personal information is transmitted. Avoid using Wi-Fi networks; they may permit interception of data.

10. Manage Use of Portable Media. Portable media, such as DVDs, CDs and USB “flash drives,” are more susceptible to loss or theft. This can also include smartphones, MP3 players and other personal electronic devices with a hard drive that ‘syncs’ with a computer. Allow only encrypted data to be downloaded to portable storage devices.

These recommendations are general guidelines and are not intended to be exhaustive or complete nor are they designed to replace information or instructions from the manufacturer of your equipment.

© 2017 The Hartford Steam Boiler Inspection and Insurance Company. All rights reserved.