business resource center

Best Practices for Securing Personal Information Checklist

We are committed to assisting you in managing your business's loss exposures. The following checklist will help you identify areas that may need improvement and reduce the frequency and severity of data breaches.

Search and Destroy

- ☐ Inventory all devices and data, and destroy personal information that does not serve a business need
- ☐ Establish parameters for the amount of time personal information will be stored
- ☐ Avoid using social security numbers as identifiers of employees or customers; ask the same of your health insurance providers
- ☐ Use cross cut paper shredders for disposal of credit card slips or other personal information
- ☐ Wipe all data from computers, diskettes, mobile phones, tablets, USB storage media and CD-ROMS before disposal

Install Security Software

- ☐ Use and regularly update anti-virus, anti-spam, endpoint detection and response, and intrusion detection software on individual computers as well as servers
- ☐ Use and regularly update a firewall for websites and all devices with Internet connectivity
  - ☐ Establish electronic audit trails to monitor who is accessing data
  - ☐ Implement SSL (Secure Sockets Layer) / TLS (Transport Layer Security) on your website
  - ☐ Use deactivation software for mobile devices
- ☐ Encrypt (minimum 128 bits) personal information stored on computers, disks and mobile devices or sent over public networks including via email.
  - ☐ Use minimum WPA2 encryption for wireless devices

Additional Security Procedures

- ☐ All merchants accepting payment cards are required to be compliant with Payment Card Industry Data Security Standards (PCI DSS)
- ☐ Develop a privacy and data security policy including guidance on the use and storage of personal information on mobile devices
- ☐ Develop a social networking policy addressing what is acceptable to post on social media
- ☐ Develop an acceptable use policy addressing allowable usage of company devices, information and the internet
- ☐ Use multi-factor authentication for access to critical resources, whether remote or not
- ☐ Conduct annual security awareness training
- ☐ Restrict access to data on a "need-to-know" basis
- ☐ Conduct criminal or civil background checks on employees with access to personal information
- ☐ Store employee personal information in locked cabinets
- ☐ Assign a unique ID to each person with computer access to personal information
- ☐ Require multi-factor authentication (password plus token) when using remote access to your network
- ☐ Implement and regularly change strong passwords to include a mix of numbers and upper and lower case letters for both PCs and mobile devices
- ☐ Disable access by terminated employees as soon as possible
- ☐ Backup necessary personal information offsite as soon as possible to avoid losing it to cyber extortion
- ☐ Avoid sending personal information using wi-fi hotspots (i.e. hotels, airports, coffee shops)