BRC business resource center

BEST PRACTICES FOR SECURING PERSONAL INFORMATION CHECKLIST

We are committed to assisting you in managing your business' 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 and CD-ROMS before disposal

INSTALL SECURITY SOFTWARE

- ☐ Use and regularly update anti-virus, anti-spam 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 the use of the Internet
- ☐ 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 two-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
- ☐ Backup necessary personal information offsite to avoid losing it to cyber extortion
- ☐ Avoid sending personal information using wi-fi hotspots (i.e. hotels, airports, coffee shops)

BRC business resource center

BEST PRACTICES FOR SECURING PAYMENT CARD INFORMATION CHECKLIST

We are committed to assisting you in managing your business' loss exposures. All merchants accepting payment cards are required to comply with Payment Card Industry Data Security Standards (PCI DSS). Are you in compliance? Use our checklist below.

- ☐ Build and maintain a secure network including installation and maintenance of firewalls, antivirus and encryption
- ☐ Use strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open public networks
- ☐ Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network
- ☐ Maintain and disseminate a policy that addresses information security for all personnel
- ☐ Avoid storage of cardholder data if possible; if stored, limit retention time to that required by business, legal and/or regulatory purposes
- ☐ Implement strong access controls including limiting access to those whose job requires such access, strong passwords and secure storage areas
- ☐ Assign a unique username to each person with computer access
- ☐ Employ two factor authentications for remote access to the network by employees, administrators and third parties
- ☐ Render all passwords unreadable during storage and transmission by using strong cryptography
- ☐ Monitor and test your network, security systems and processes regularly
- ☐ Verify third party service providers are PCI DSS compliant when outsourcing any part of your IT infrastructure
- ☐ Change default passwords for POS systems and other Internet-facing devices before installing on a network
- ☐ Utilize a checkout or payment page hosted by a PCI DSS compliant service provider to process customer online payment information outside your own business network
- ☐ Implement a tokenization solution when processing payment cards yourself to enable repeat online customers to securely store and access their payment information
- ☐ Never store sensitive authentication data after authorization when processing payment cards; this includes sensitive data that is printed on a card or stored on a card's magnetic stripe or chip, and personal identification numbers entered by the cardholder
- ☐ Contractually commit third party vendors to compliance with PCI requirements and include indemnity requirements when a breach happens