

MerchantResource



The Payment Card Industry Data Security Standard: Physical Security

Did You Know?

In 2005, U.S. organizations reported that virus attacks, unauthorized access, and stolen laptops and other mobile technology resulted in the first, second and third largest financial losses, respectively, in regards to data compromises.* In pursuit of a secure computer network, organizations often focus on technology solutions and neglect more traditional security controls, such as stowing laptops in lockable cabinets at the end of the day.

While a majority of the PCI DSS call for a variety of technology solutions, traditional security measures should also be enforced. Sound data security policies require both digital and physical security measures. This information sheet provides advice on implementing physical security standards at your organization.

To Get Started

Remember, incorporating the information below into your data security policy alone will not make you PCI DSS compliant. These tips serve as general recommendations to help you establish physical security standards.

To help merchants better secure their networks and work toward PCI compliance, Chase Paymentech partnered with AmbironTrustWave, a compliance management and data security expert, to provide the expertise you need.

AmbironTrustWave works with thousands of merchants, from mom-and-pop shops to global operations, guiding them through the PCI DSS compliance process.

AmbironTrustWave's TrustKeeper®

AmbironTrustWave's TrustKeeper® is an easy-to-use Web portal that helps merchants complete the PCI DSS Self-Assessment Questionnaire, schedule required scans, manage onsite audits and answer the questions they have about their network environment and PCI DSS compliance.

To get started, visit

<http://www.chasepaymentech.trustkeeper.net>

If you have any questions, please contact AmbironTrustWave support at 1-888-878-7817.

CHASE  Paymentech™

* According to the 2006 CSI/FBI Computer Crime and Security Survey conducted by the Computer Security Institute in cooperation with the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad
(see: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml)

First Steps

To jumpstart your organization's physical security policy, consider the following:

Inventory

Protect your assets by first accounting for them. Inventory your organization's technology and note employee possession and responsibility of individual items, such as:

- Laptop computers
- Desktop computers
- Servers
- Any other technologies
- Any other physical assets
 - Hardcopy contracts
 - Hardcopy tax forms
 - Payment card receipts

Identify and Secure

Once you've recorded what your organization owns, secure those assets by:

- Engraving or affixing asset tags to laptops
- Locking desktops to desks
- Instituting a policy requiring laptops be locked away at the end of the business day
- Ensuring your computer server/data center is located in a locked room
- Using lock boxes or locking file cabinets to store sensitive hardcopy documents

Take care to only grant asset access (permissions, keys, etc.) to employees that have business "need to know." And note which employees have access to what assets.

Monitoring

As the PCI DSS require auditing and logging of digital access to your computer network, it requires the same of the physical access to areas where cardholder data is stored or transmitted. These areas can include:

- Computer rooms with servers involved in the payment card acceptance chain
- Payment card receipt storage rooms
- Mail order processing areas

To ensure security:

- Install cameras at entry/exit points.
 - Monitor cameras regularly and keep cameras' recorded data for at least three months.
- Require ID badges for individuals with access to sensitive data centers.
- Use a visitor's log for sensitive facility areas.
 - Recording who accessed areas can help determine cause and liability in a data security incident.

Policies and Procedures

PCI DSS require a commitment from every employee; however, employees must be educated about their organization's security policies and practices. Communicate your policies and procedures to employees, which should include:

- External and internal distribution of media that contains cardholder data
- Destruction of media that contains cardholder data or other sensitive data
- Restricted versus non-restricted areas
- Distinguishing visitors from employees (and approved visitors areas)
- Care and proper usage of organization computers, cell phones, etc.