PCI Best Practices

Last Revision Date: April 6, 2023

Best Practices:

1. If You Don't Need It, Don't Store It!

- Keep cardholder data storage to a minimum. Limit storage amount and retention time to only that which is required for legal, regulatory, and/or business requirements. Many offices retain cardholder data (CHD) "just because" or there is often a misconception this information is needed for "recurring" payments. If data is not absolutely necessary in order to conduct business, do not retain it in any format. If you retain the transaction number and date, you can always ask the acquiring bank for the cardholder data if requested.
- This includes all paper and forms. Once a transaction has been processed, destroy all CHD on the form. This may require a redesign of the form to move the CHD to the bottom where it can be properly removed and cross-cut shredded.

2. Eliminate Electronic Storage of CHD

- Do not copy or type CHD into spreadsheets or documents on general use workstations even for temporary use. Even if you don't save the document, an image or file of the data is stored on the hard drive. Portable electronic media devices should not be used to store cardholder data, including, but not limited to, the following: laptops, compact discs, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.

3. Implement Proper Destruction Methods

- All forms or paper with cardholder data should be shredded in a cross-cut or finer shredder.
- Third-party shredding services may be used, as long as the bins provided are secure and cannot be removed from the area.

4. Use Online Payment Card Systems Appropriately

- Many departments use third-party payment systems or gateways to outsource online payment card processing. Customers should be directed to complete payments online using these applications. If you are specifically directing people to use computer labs, kiosk machines, or other public-use computers to make payments, this can inadvertently bring these devices into your PCI scope. Do not direct customers or offer payment card entry on any device that has not been properly secured or approved by your PCI Team.
- Often staff members are under the impression that it is considered good customer service to take phone calls, emails, or some other form of communication to process a credit card transaction for a customer, however:.

o It is not recommended to act as the customer and input their data for them.

o When it is necessary to provide this service: do not use a general-purpose workstation; transactions should be conducted on a separate (segmented) payment terminal.

5. Never Email Credit Card Information

- Staff should never use email as a manner of receiving or transmitting cardholder data.
- Implement a formal policy denying the use of e-mail for payment acceptance across the institution and train all staff on what to do if they receive an e-mail with payment card details.
- Should a customer email their payment card information:

o Reply to the sender, deleting the credit card information from the reply and inform them that "for their protection and that of {INSTITUTION NAME}, policies dictate that payment card information shall not be accepted via email. Please use one of our accepted methods of processing your information: (in-person, online, fax, form, etc.)."

6. Maintain Clean Desk Policy

- CHD should not be left out on desks or in plain sight. Even if leaving the desk for a short period, staff should keep material in a folder and lock the folder in a secure location. At the end of the day, all CHD should be stored in a secure file cabinet or safe. Always log out or lock your computer when it is unattended.

7. Limit and Monitor Physical Access to Systems That Store, Process or Transmit Cardholder Data.

- If physical access is not restricted, malicious individuals could easily get their hands on sensitive data. Do not allow unauthorized persons unaccompanied access to areas where credit card data is stored or processed. This includes other {INSTITUTION NAME} staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This could potentially require a change in service times.
- Identify onsite personnel and visitors with badges and revoke badges upon termination or completion of visit.
- Keep a visitor log to maintain a physical audit trail of visitor activity, documenting the visitor's name, firm represented and the onsite personnel authorizing access.

8. Secure the Processing Environment

- The threat of Point of Sale (POS) terminal tampering is serious, as every day criminals attempt to install skimmers and other devices to capture cardholder data and create fraudulent cards. Ensure all POS devices are secure and periodically inspect devices for tampering and/or substitution.
- Keep an inventory of all devices (with serial numbers) and train staff to look for abnormalities (broken seals, damage to the device, damage to external cables, etc.).
- You should also train staff to limit access to POS devices to only authorized individuals. Report any third-party individuals claiming to be repair or maintenance personnel immediately.

9. Document Desk Procedures

- To ensure continuity across the institution, require all individuals to document daily procedures, and their roles and responsibilities for handling of cardholder data. Include such items as receipt and processing procedures, disposition and destruction of CHD, and storage and transfer of forms within the office.

10. Keep Duties Related to Processing Cardholder Information as Separate Roles (i.e. issuing refunds, processing receipts, etc.)

- Implement basic policy, documented processes, and systems that enforce access and restriction of access to any systems that store, process or transmit cardholder data. Only those with a legitimate business need to access the information should be given privileges. Establish and define job roles and only provide access to the least amount of data needed to carry out individual responsibilities.

- Separation of duties is an internal control, and the concept of having more than one person required to complete a task to prevent wrongful acts, fraud, abuse and errors. This can also help ensure any potential incidents are detected.

11. Improve Oversight of Third-Party Service Providers

- You cannot completely outsource your PCI compliance responsibility. It is important that you know and document all third-party service providers involved in payment card processing. It is also critical to ensure the appropriate contractual language is in place dictating which specific PCI DSS requirements are the responsibility of each entity.
- Assessing these vendors and service providers annually will ensure their compliance efforts are sufficient and protect your institution from any collateral damage should they suffer a data breach.

12. Implement a Formal Incident Response Plan

- Create a comprehensive incident response plan pertaining to cardholder data breaches and train all staff to report any suspicious incidents immediately. If you ignore the warning signs of a potential security breach or fraud, it could cost the organization valuable time and resources.

13. Implement Security Awareness Training

- Educating your staff (and third-parties) on general information security best practices can go a long way in preventing expensive mistakes due to human error. Training on the PCI DSS and general information security for all staff (including topics like social engineering, phishing, password management, etc.) must be provided to all staff members with access to cardholder data upon hire, and at least annually thereafter.