The Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that were created to guarantee the protection of cardholder data during payment card transactions. It was developed by major credit card companies, including Visa, Mastercard, American Express, Discover, and JCB. The creation of this framework is for securing sensitive information and mitigating the risk of data breaches and fraud.

The PCI DSS framework is made up of 12 high-level requirements. Compliance with these standards is mandatory for any organization that processes, stores, or transmits payment card information. The 12 requirements are the following:

1. Install and maintain a firewall configuration to protect cardholder data- Implement a firewall to secure your network from unauthorized access and protect cardholder data.
2. Do not use vendor supplied default passwords or settings- Change your default passwords and other security settings provided by vendors for systems, applications, and network devices, preventing potential unauthorized access.

3. Protect stored cardholder data- When cardholder data is stored it must be encrypted for protection against unauthorized access.

4. Encrypt transmission of cardholder data across open public networks- Use strong encryption methods to protect cardholder data during transmission over public networks.

5. Use and regularly update anti-virus software or programs- Install and maintain anti-virus software on all systems commonly affected by malicious software. Regularly update the software and perform scans to detect and remove any malware.

6. Develop and maintain secure systems and applications- Ensure that systems and applications are developed and maintained securely. Implement secure coding practices, perform regular vulnerability assessments, and patch systems promptly.

7. Restrict access to cardholder data by business need to know- Limit access to cardholder data to only those individuals with a legitimate business need. Assign unique IDs to each user and implement strong access controls.

8. Assign a unique ID to each person with computer access- Ensure that each user has a unique identifier when accessing systems and cardholder data. This helps with accountability and tracking of user actions.

9. Restrict physical access to cardholder data- Protect physical access to areas where the cardholder data is stored or processed. Use access controls, surveillance systems, and secure physical storage methods.

10. Track and monitor all access to network resources and cardholder data- Implement logging mechanisms and review logs regularly to detect and respond to suspicious activities. Use time synchronization and secure log storage.

11. Regularly test security systems and processes- Conduct regular security testing, including vulnerability scans and penetration testing, to identify and address vulnerabilities. Perform tests after significant changes to systems or applications.

12. Maintain a policy that addresses information security for all personnel- Develop and maintain an information security policy that addresses all aspects of PCI DSS compliance. Regularly educate personnel about the policy and their security responsibilities.

Non compliance with the PCI DSS standards can result in fines or penalties. Some penalties include Increased transaction fees, regulatory fines from the government and the loss of card processing privileges. Some ways to satisfy regular compliance with PCI DSS include the following:

1. Encryption- Use encryption techniques to protect cardholder data
2. Network segmentation- Split up networks to help isolate cardholder data, reducing the risk of unauthorized access.
3. Vulnerability management- Scanning systems and applications regularly to check for vulnerabilities, safeguarding them from potential exploits.
4. Incident response- Create a incident response plan that addresses potential security breaches
5. Compliance Documentation- Have proper documentation of security policies, procedures and controls to comply with the PCI DSS requirements.

The PCI DSS applies to all organizations that process, store, or transmit payment card information. This means that non-profit organizations that handle payment card data must meet the requirements for compliance.Non-profit organizations often accept payment cards for various purposes, such as donations, membership fees and event registrations. These organizations become responsible for protecting the confidentiality, integrity, and availability of cardholder information.

Compliance with the PCI DSS helps non-profit organizations secure cardholder data and reduce the risk of data breaches and fraud. Compliance with the PCI DSS requirements is necessary for maintaining the trust of donors and members.

PCI DSS Quick ReferenceGuide
https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Auditboard.com

https://www.auditboard.com/blog/pci-dss-requirements/#:~:text=The%2012%20requirements%20of%20PCI%20DSS%20compliance%20are%20designed%20to,vulnerability%20management%20program%2C%204)%20%E2%80%8B

Official PSI Security Standards website
https://www.pcisecuritystandards.org/about_us/