Resource

Diamond Mind®

Understanding the 12 Tenets of PCI-DSS Security

Becoming compliant with Payment Card Industry Data Security Standard (PCI-DSS) requires 12 steps to upgrade school networks and strengthen physical security operations. Use this guide to safeguard your systems, ensure compliance, and build trust with families.

1. Establish Network Security Controls

- Protect cardholder data and transaction details with a firewall that blocks unknown or suspicious users.
- Implement network segmentation to isolate payment systems from the rest of the network, reducing exposure to potential threats.

2. Strengthen Logins Across the School

- Passwords should include numbers, symbols, and 12 or more characters and never remain the default or temporary login a software vendor provides for initial access.
- Employee onboarding is the crucial phase to introduce cybersecurity best practices, especially for financial and IT teams working directly with sensitive payments information and processing.
- Multi-factor authentication gives your school an extra layer of protection with users needing access to their personal phone to login via a unique code sent to their text or email.

3. Encrypt Stored Cardholder Information

- Convert sensitive financial and student information into a coded format that is unreadable without a decryption key.
- A secure key management system can generate, rotate, and revoke keys while storing them separately from the data they encrypt.
- Apply encryption to all stored financial data, including databases, backups, and log files.

4. Encrypt Transmission of Cardholder Data

- Encrypt data before it leaves the sender and ensure it gets decrypted only when in the hands of the intended recipient.

5. Protect Systems Against Malware

- Schools should implement and regularly update antivirus and anti-malware software on all devices that handle or access payment data.

VenturEd Solutions™

6. Maintain Secure Systems and Applications

- Regularly patch operating systems, software, and payment applications to fix known security vulnerabilities.
- Third-party apps should only be used if they meet security standards.

7. Enforce Strict Access Controls

- Access to confidential data should be strictly controlled and limited to authorized personnel only.
- Firewalls must be properly configured and maintained to monitor and block unauthorized access.
- Allocate role-based permissions according to business need-to-know.

8. Ensure Individual, Authenticated Access

- Assign unique user IDs and require strong passwords or multi-factor authentication for anyone accessing sensitive systems.
- Each individual should have their own account—no shared or team accounts.

9. Protect Physical Spaces

- Physically secure all devices holding cardholder information, including server rooms, POS terminals, and workstations, with access restricted to authorized personnel only.
- Periodically train remote and hybrid employees on best practices to secure school laptops within their homes.

10. Track and Monitor All Network Access

- Schools should implement logging systems that record who accessed what data and when, especially within environments that handle or store payment information.

11. Routinely Test Security Systems and Procedures

- Perform regular vulnerability scans, penetration testing, and system audits to remain compliant and identify areas of weakness to address.
- Schools should also test their response plans, such as how quickly staff can react to a breach or suspicious behavior.

12. Document Security Policies

- Outline how data is protected, who is responsible for maintaining security, and what steps should be taken in the event of a breach.