Payment Card Industry Data Security Standard (PCI DSS):
This is an information security standard that applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers (PCI Security Standards Council, 2021).

It was developed to enhance cardholder data security and to ensure the safe handling and storage of sensitive customer credit card information and data (PCI Security Standards Council, 2021).

Main Components of PCI DSS:

1. Build and Maintain a Secure Network and Systems
    - Install and maintain a firewall configuration to protect cardholder data.
    - Do not use vendor-supplied defaults for system passwords and other security parameters.
2. Protect Cardholder Data
    - Protect stored cardholder data.
    - Encrypt transmission of cardholder data across open, public networks.
3. Maintain a Vulnerability Management Program
    - Protect all systems against malware and regularly update anti-virus software or programs.
    - Develop and maintain secure systems and applications.
4. Implement Strong Access Control Measures
    - Restrict access to cardholder data by business need-to-know.
    - Identify and authenticate access to system components.
    - Restrict physical access to cardholder data.
5. Regularly Monitor and Test Networks
    - Track and monitor all access to network resources and cardholder data.
    - Regularly test security systems and processes.
6. Maintain an Information Security Policy
    - Maintain a policy that addresses information security for all personnel (PCI Security Standards Council, 2021).

Policy Behind the Creation of PCI DSS

- The PCI DSS was developed in 2004 by the founding payment brands of the PCI Security Standards Council, namely, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.
- The key policy reason behind its creation was to consolidate the various industry data security standards into one unified framework to manage the ongoing evolution of the Payment Card Industry (PCI) security standards (Vijayan, 2007).

References:
PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf

Vijayan, J. (2007). Q&A: New security standards council aims to 'take PCI to the next level.' Computerworld. Retrieved from https://www.computerworld.com/article/2544689/q-a--new-security-standards-council-aims-to--take-pci-to-the-next-level-.html

TKH & PCI DSS

If a medium-sized non-profit organization accepts credit or debit card donations through its website, then it is indeed involved in payment card processing, and so it must comply with the Payment Card Industry Data Security Standard (PCI DSS).

How the requirements of PCI DSS could apply to The Knowledge House:

- Build and Maintain a Secure Network and Systems: The non-profit organization needs to ensure that its donation processing system is secured by firewalls, and that all default passwords provided by vendors (for instance, for servers or software systems) are changed.
- Protect Cardholder Data: The organization should never store sensitive cardholder data unless absolutely necessary, and if it is stored, it should be encrypted or otherwise protected. Data that is transmitted (such as to payment processors) should always be encrypted as well.
- Online Donations: If the non-profit organization is accepting donations online through their website and these donations are processed using a credit or debit card, they are required to be compliant with PCI DSS (Williams, 2016).
- Cardholder Data Security: The non-profit must ensure that it is securely handling and storing any cardholder data that it collects during the donation process. This includes encryption of data both in transit and at rest, as well as secure disposal of data when no longer required (PCI Security Standards Council, 2021).
- Third-Party Processors: If the non-profit uses a third-party payment processor, the organization is still responsible for ensuring the processor is PCI compliant. While the processor will handle much of the technical and operational aspects of card data security, the non-profit has an obligation to ensure their service providers also adhere to PCI DSS (Jones, 2020).
- Regular Audits: Non-profits accepting card payments are required to conduct regular PCI DSS audits, which could be an annual or quarterly process depending on the organization's transaction volume. These audits should be performed by a Qualified Security Assessor (QSA) or an Internal Security Assessor (ISA) (PCI Security Standards Council, 2021).
- Data Breach Liability: In the event of a data breach, a non-profit organization can be held liable for the financial losses resulting from the breach if it is found to be non-compliant with the PCI DSS at the time of the breach (Fenton, 2018).

References:

Williams, K. (2016). The ABCs of PCI Compliance for Nonprofits. Network for Good. Retrieved from https://www.networkforgood.com/nonprofitblog/pci-compliance-nonprofits/

Jones, C. (2020). What is PCI Compliance and Why It's Important for Your Business. Business News Daily. Retrieved from https://www.businessnewsdaily.com/10930-pci-compliance.html
Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf

Non Compliance of PCI DSS

- Fines and Penalties: Non-compliance with PCI DSS can lead to monetary penalties. These are usually levied by the credit card companies themselves and can range from $5,000 to $100,000 per month. The actual amount depends on the size of the organization, the duration of non-compliance, and the number of transactions processed (Gibson, 2018).
- Card Replacement Costs and Forensic Audits: If a breach occurs and the organization is found to be non-compliant, they could be responsible for the costs associated with replacing compromised cards and conducting forensic audits to determine the cause and extent of the breach (Gibson, 2018).
- Increased Transaction Fees: Merchants who are not PCI compliant may face increased transaction fees from their banks or payment processors (Gibson, 2018).
- Reputation Damage: Data breaches can significantly damage an organization's reputation. For a non-profit, this could mean a decrease in donations as donors lose trust in the organization's ability to safeguard their data (Fenton, 2018).
- Loss of Credit Card Privileges: In severe cases, the non-profit could lose the ability to accept credit card payments altogether, which could significantly impact its ability to raise funds (Williams, 2016).

References:

Gibson, S. (2018). The Real Cost of PCI DSS Non-Compliance. SecurityMetrics. Retrieved from https://www.securitymetrics.com/blog/real-cost-pci-dss-non-compliance

Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk

Williams, K. (2016). The ABCs of PCI Compliance for Nonprofits. Network for Good. Retrieved from https://www.networkforgood.com/nonprofitblog/pci-compliance-nonprofits/

How a Secure Program Keep TKH in PCIDSS Compliance

1. Secure Cardholder Data: The program should ensure that all cardholder data is securely stored and transmitted. This includes encryption of data both in transit and at rest, secure disposal of data when no longer required, and minimization of stored data (PCI Security Standards Council, 2021).
2. Use of Firewalls: Implement and maintain firewalls to protect internal networks from unauthorized access. These firewalls should be properly configured and updated regularly (SANS Institute, 2015).
3. Maintain a Secure Network: This involves changing vendor-supplied defaults, maintaining a vulnerability management program, and developing and maintaining secure systems and applications (PCI Security Standards Council, 2021).
4. Access Controls: Implement strong access control measures. This includes limiting access to cardholder data to those with a business need-to-know, implementing strong user authentication methods, and controlling physical access to systems (PCI Security Standards Council, 2021).
5. Regular Monitoring and Testing: Regularly monitor and test networks to identify and rectify any vulnerabilities or breaches. This includes tracking and monitoring all access to network resources and cardholder data, as well as regularly testing security systems and processes (PCI Security Standards Council, 2021).
6. Information Security Policy: Maintain a robust information security policy that is communicated to all personnel. This should outline all security measures, responsibilities, and expectations in relation to cardholder data security (SANS Institute, 2015).

References:

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf

SANS Institute. (2015). A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS). Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/practical-guide-payment-card-industry-data-security-standard-pci-dss-35962