***What is PCI Compliance?***

Due to growing concerns with credit card fraud and widely publicized security breaches involving cardholder data, the credit card industry established new standards called Payment Card Industry Data Security Standard (PCI DSS, but often referred to as just PCI compliance).

These requirements cover a wide assortment of practices, technology, and systems and can be very complex to understand, let alone comply with. Primarily they relate to how your organization handles, stores, and transmits cardholder data. Here are a few of the most important elements:

- Never store CVV2 data (the 3-digit code on the back of the cards) or magnetic strip data.
- If credit card numbers need to be stored or transmitted, they should generally be encrypted with a least 128-bit encryption.
- Restrict access to physical and electronic cardholder data with user-specific passwords and based on business need-to-know guidelines.

More complete information on the PCI DSS can be found at www.pcisecuritystandards.org

***PCI Compliant Donations***

Stewardship's suite of payment processing tools is audited every year for compliance to PCI standards and is currently compliant at Level 1 PCI DSS, the highest level of compliance.

***Does this apply to my nonprofit?***

Every organization that accepts credit cards is required to comply with PCI DSS, but the requirements for compliance can vary widely depending on the types of processing you do and the volume of credit card transactions processed. Merchants fall into one of four levels. Most nonprofits fall into the lowest processing volume category (Level 4 with less than 20,000 Visa/MC transactions per year), where the primary requirement is the completion of a PCI self-assessment questionnaire and quarterly network scans. Although PCI certification for Level 4 merchants is not required by all acquirers, effective July 1, 2010 there is a mandate to use PA-DSS compliant payment applications. Stewardship clients are outside the scope of this mandate since all data hosted on our system and in our servers is certified PCI compliant.