How can YOU protect cardholder data?

The University's policy is to never store credit card data electronically.

If you use Payment Card readers that transmit and receive Cardholder Data and/or store Cardholder Data on paper, **you must comply** with the following requirements:

1. During business hours, restrict cardholder data to a controlled-access area. After business hours, keep cardholder data in a locked container (file cabinet, safe, vault). Only those who have a business need to access cardholder data should have keys, combinations, and other access to the data.

2. Dispose of Cardholder Data in a secure manner as your business need for it expires. For example, use a cross-cut shredder or shredding service.

3. Full electronic cardholder credit card numbers must ***never*** be stored. Partial numbers may be stored for a limited time, but must be truncated to the last 4 digits.

4. Never retain the cardholder verification values or codes (CVV codes).

5. Do not store the PIN or the full contents of any track from the magnetic stripe.

6. Do not allow donors, vendors etc. to email credit card numbers. Have them call and provide the number over the phone instead. If the credit card number is written down, it MUST be destroyed as soon as possible.

7. Merchants should regularly inspect their point–of-sale terminals (front and back) to ensure they have not been tampered with. This includes checking to see if the serial number is correct and that the Ethernet cable goes directly to the wall jack with no intermediate devices attached.