Best Practices to Handle Payment Card Data Securely

If you are responsible for processing, transmitting, storing, or accessing payment card data, follow these payment card data security best practices to protect the cardholder, your department or unit, and the University.

If You Handle Card-Present Transactions

A card-present transaction is when the cardholder presents the payment card in person for a face-to-face transaction and swipes, inserts, or taps the card at a terminal or point-of-sale (POS) system.

- ✓ Keep the payment card within the customer’s view.
- ✓ Shield the customer's payment card data from the view of others.
- ✓ Ask the customer to enter their Personal Identification Number (PIN) for a debit transaction. Never ask for a cardholder's PIN.
- ✓ Do not retain or store the payment card expiration date, verification number, or security code on any transaction documents, on paper, or in any electronic system.
- ✓ Record only the last four digits of the payment card account number on any department receipts, invoices, data in electronic systems, and documentation that is distributed outside the unit.
- ✓ Keep documents containing payment card information in secure storage mechanism (such as a locked file cabinet or safe) in a restricted, secure area.
- ✓ Make documents that contain cardholder data unreadable (such as by cross-cut shredding) before discarding them.

If You Handle Card-Not-Present Transactions

A card-not-present transaction is when the payment card data is manually entered by the merchant for an order by mail, phone, or fax; or by the customer at an Internet site.

- ✓ Do not send or accept payment card information by email.
- ✓ Do not retain or store the payment card expiration date, verification number, or security code on any transaction documentation, on paper or in any electronic system.
- ✓ Design your registration or order forms so that card data can be easily removed and shredded after the payment has been processed for authorization (such as a perforated bottom of a form).
- ✓ Record only the last four digits of a payment card account number on any departmental receipts, invoices, data in electronic systems, and documentation that is distributed outside the unit.
- ✓ Keep documents containing payment card information in secure storage mechanism (such as a locked file cabinet or safe) in a restricted/secure area.
- ✓ Make documents containing cardholder data unreadable prior to discarding them (such as by cross-cut shredding).