

Michigan State University PCI-DSS Exit

Card Data covered by PCI-DSS includes (Select all answers that apply):

- Merchant Name and Address
- PAN (Full credit card number)
- CVV (Card Validation Verification number)
- Cardholder Name
- Merchant Banking Account Details

SUBMIT

Menu

- 13.1. Risks
- 13.2. Social Media
- ▼ 14. Testing
 - 14.1. Testing
- ▶ 15. Policies
- ▼ 16. Quiz
 - 16.1. Card Data covered by PCI-DSS includes (Select all answers that apply):
 - 16.2. PCI-DSS assumes that the following methods of cardholder data transmission are risky (Select all answers that apply):
 - 16.3. Choose which of the below must be followed by merchants at POS terminals for PCI-DSS compliance? (Select all answers that apply):
 - 16.4. Mix'n'Match

Search...

Guidance: Merchant information such as Name, Address, and Banking Account details are not considered Cardholder Data.

Michigan State University PCI-DSS Exit

PCI-DSS assumes that the following methods of cardholder data transmission are risky (Select all answers that apply):

- Encrypted electronic communications
- Private Email
- All http:// web sites
- Telephone calls to close friends.
- Signed FedEx Courier of unencrypted electronic data
- Social Media sites
- IMs & SMS & MMS with known associates.

SUBMIT

Menu

- 13.1. Risks
- 13.2. Social Media
- ▼ 14. Testing
 - 14.1. Testing
- ▶ 15. Policies
- ▼ 16. Quiz
 - 16.1. Card Data covered by PCI-DSS includes (Select all answers that apply):
 - 16.2. PCI-DSS assumes that the following methods of cardholder data transmission are risky (Select all answers that apply):
 - 16.3. Choose which of the below must be followed by merchants at POS terminals for PCI-DSS compliance? (Select all answers that apply):
 - 16.4. Mix'n'Match

Search...

Guidance: Encrypted communications are the only method of data transmission that is considered less risky or not risky by PCI-DSS.

Michigan State University PCI-DSS Exit

Choose which of the below must be followed by merchants at POS terminals for PCI-DSS compliance? (Select all answers that apply):

- Look for added skimmers or card reader
- Never let the customer see the POS
- Look for signs of hacking
- Check the POS for normal operation
- Power down the POS when not in use
- Always use the POS-vendor-supplied passwords.
- Examine customer receipts for accuracy and compliance

MICHIGAN STATE UNIVERSITY

Menu

- 13.1. Risks
- 13.2. Social Media
- ▼ 14. Testing
 - 14.1. Testing
- ▶ 15. Policies
- ▼ 16. Quiz
 - 16.1. Card Data covered by PCI-DSS includes (Select all answers that apply):
 - 16.2. PCI-DSS assumes that the following methods of cardholder data transmission are risky (Select all answers that apply):
 - 16.3. Choose which of the below must be followed by merchants at POS terminals for PCI-DSS compliance? (Select all answers that apply):
 - 16.4. Mix'n'Match

Search...

◀ ▶

↻
SUBMIT

Guidance: Merchants should follow their departments business procedures while operating the POS (Point of Sale) device. Procedures should include routine inspection of devices for skimmers, signs of hacking, normal operation, and normal customer receipts.

Michigan State University PCI-DSS Exit

Mix'n'Match

Wireless	User and card data after use
Passwords	Keeping card data secret.
Confidentiality	Hard to Guess - Easy to Remember
User_IDs	Unique
Destroy	Always employ encryption

MICHIGAN STATE UNIVERSITY

Menu

- 13.2. Social Media
- ▼ 14. Testing
 - 14.1. Testing
- ▶ 15. Policies
- ▼ 16. Quiz
 - 16.1. Card Data covered by PCI-DSS includes (Select all answers that apply):
 - 16.2. PCI-DSS assumes that the following methods of cardholder data transmission are risky (Select all answers that apply):
 - 16.3. Choose which of the below must be followed by merchants at POS terminals for PCI-DSS compliance? (Select all answers that apply):
 - 16.4. Mix'n'Match
 - 16.5. Thank You

Search...

◀ ▶

↻
SUBMIT

Guidance:

- Encryption should always be used with wireless connections.
- Passwords should never be easy to guess, only easy for the proper user to remember.
- Card Data should always be kept confidential and secret.
- It is MSU Policy that User ID's are Unique.
- After use, Card Holder Data should never be kept.