PCI compliance at U-M

What does PCI compliance mean?

Payment **C**ard **I**ndustry Data Security Standard (PCI DSS) compliance is a critical and mandatory aspect of securely accepting credit cards. Visa, MasterCard, Amex, and Discover collaborated to create common industry security requirements that each merchant must comply with to **safeguard sensitive credit card data**.

This applies to all payment methods, including retail, mail/telephone order, and e-commerce.

What type of merchant are you?

Depending on the method of credit card acceptance (e.g., online, terminal, PC, etc.,), a specific version of the PCI annual questionnaire will need to be completed.

Which one do you have to complete? Contact PCIcompliance@umich.edu for the version that applies to your area.

6/1/2024

Annual top 3-step PCI compliance processes

All U-M merchants must complete the following steps:

1. **Complete Merchant Certification Course in My LINC**
   A report showing who has taken the TME102 training can be found at:
   (Business Objects>Public Folders>UM Maintained> Financials>FN03>FN03 Journal Detail Merchant Management Report)

2. **Review the Merchant Requirements**
   The merchant contact reviews this document (https://www.finance.umich.edu/node/2348) to verify the all of the merchant responsibilities, including PCI compliance are being completed.

3. **Complete the PCI Compliance Self-Assessment Questionnaire (SAQ)**
   Complete the SAQ that is applicable to your unit's type of merchant(s) on the CampusGuard website by the annual deadline. CampusGuard is an online portal that manages SAQs for university merchants.

M | FINANCE
UNIVERSITY OF MICHIGAN

What’s the risk?

There are over 400 merchants at U-M processing credit card transactions.

- PCI compliance violations by even one merchant could result in fines/penalties or even the university losing the right to process credit card transactions.
- A credit card breach could jeopardize the confidence of key constituents like donors, customers, patients, employees, parents, and students.

Credit card data lost, stolen, or suspect fraud?

Immediately email full details to the Treasurer's Office at: merchantservices@umich.edu.

Wait for a response for any next steps.

PCI Compliance Resources:

https://finance.umich.edu/treasury/merchant-services/pci

Common merchant pitfalls

- Out-of-date merchant contacts in M-Pathways.
- Improper—or out-of-date—training for individuals who handle credit card data.
- Merchants not monitoring refund activity (e.g., duplicates, incorrect amounts, refunds to incorrect credit cards, etc.)
- PCI SAQ(s) not completed by annual deadline.
- Taking credit card data over the phone with the wrong type of phone.

Is your merchant information up to date?

Merchant Contacts are responsible for maintaining the authorized user list (staff who are authorized to process credit cards or handle credit card data) in M-Pathways. Instructions can be found at: https://maislinc.umich.edu/mais/html/GL_CR_Deposit_Merchant.html

Merchant Services FAQs:

https://finance.umich.edu/treasury/merchant-services