

University Cash Services

## Cash Handling

### PCI Best Practices

Bayramian Hall Lobby  
Phone: (818) 677-8000, Option 1  
Fax: (818) 677-4911  
Mail Code: 8214

#### Purpose:

Each merchant must assign a PCI contact person to monitor, document, and manage card acceptance processes and security. There are a few key things you as a merchant should do and not do to ensure you are compliant with PCI's standards. This shortlist of "Do's" and "Don'ts" should get you started down the path of PCI compliance.

#### PCI Compliance: Do's

- Supervise all visitors in areas where credit card information is maintained.
- Complete your merchant accounts annual PCI DSS certification.
- Take the required annual PCI awareness training through "Training & Professional Development" on employee portal
- Perform periodic inspections to look for tampering.
- Report immediately to your supervisor and University Cash Services if you suspect card information has been stolen, lost, exposed or otherwise misused; or if your system containing credit card data has been hacked or breached.

#### PCI Compliance: Don'ts

- Never physically write down any card information.
- Never transmit or accept any of the cardholder's information via email, fax, scan, phone, or by end-user messaging technologies (i.e, Slack).
- Never store any sensitive authentication data on university computer, server or paper.
- Never share the password to your computer or any computer your access with anyone.
- Never leave sensitive information unattended on a desk, screen or in any public area.
- Never use as a 3<sup>rd</sup> party method of payment nor use in place of a cashier.

**Timeline of Tasks:** *The timeline below outlines the tasks that must be completed by merchants, in order to satisfy the annual PCI DSS Certification*

**May to Mid-June:** All merchants & operators complete their annual PCI training.

**Beginning of July:** University Cash Services (UCS) sends eMarket/operator Audit.

**Mid to End of July:** Merchants/Operators respond to UCS's audit.

**Beginning of December:** University Cash Services (UCS) sends eMarket/operator Audit.

**Mid to end of December:** Merchants/Operators respond to UCS's audit.

**EMPLOYEE ACKNOWLEDGEMENT**

I certify that I have read and received a copy of the PCI Best Practices and fully understand my responsibilities with respect to what is outlined by University Cash Services.

Name \_\_\_\_\_

Dept: \_\_\_\_\_ Ext: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_