

Miami University
CREDIT CARD SECURITY POLICIES AND PROCEDURES

Many departments on campus process credit card transactions, either infrequently or in the course of daily business. It is important that we protect the privacy of our customers, as well as maintain compliance with the Graham Leach Bliley (GLB) Act* and the Payment Card Industry Standards (PCI)**.

If your department transacts business using credit cards or wishes to, please contact the Office of Treasury Services (9-7020) to coordinate account set-up and banking arrangements. In addition, please follow the guidelines described below for the processing of credit card transactions. Adhering to the following procedures will help insure the integrity and security of all credit card transactions.

- Credit card transactions must be in person, by telephone, by mail, or via a secure university approved internet or firewall-protected and encrypted database application (Cashnet is an available provider of this service – contact the Office of the Bursar for more information). Do not accept credit card information via email, or send such information to another department via email.
- Printed customer receipts that are distributed outside the department must show only the last four digits of the credit card number.
- If you store paper records containing credit card numbers, all but the last four digits should be redacted within 60 days, or as soon as refunds or disputes are no longer likely, but no more than 180 days. Do not store credit card information in a customer database or electronic spreadsheet. Paper records must be stored in a locked room or cabinet, to which only authorized employees are permitted access.
- Retain the original receipts (displaying only the last 4 digits of the account number) and signed documentation for four years, in accordance with the University's records and retention guidelines.

Since the University could face penalties for failing to comply with the PCI** credit card industry standards to protect cardholder data, you must begin following the procedures above immediately. Failure to do so may result in your department being asked to discontinue the practice of accepting credit cards.

If you feel that credit card records may have been compromised in any way, whether through malicious intent or due to a weakness in the handling and processing of credit card transactions, please notify the Office of the Bursar (9-8700), Treasury Services Office (9-7020), or the University Information Security Office (9-9252) immediately.

*Graham-Leach-Bliley Act may be viewed online at: <http://www.ftc.gov/privacy/glbact/>

**Payment Card Industry Standards may be viewed online at http://usa.visa.com/download/business/accepting_visas_ops_risk_management/cisp_PCI_Data_Security_Standard.pdf?it=search

