GIFT ACCOUNTING

Credit Card Processing Guidelines

PCI-DSS Standard

Auburn University has an obligation to protect cardholder data and must comply with the standards set forth by the Payment Card Industry Data Security Standards (PCI-DSS.) Because Gift Accounting accepts credit cards for payment, credit card data must be securely protected. The following guidelines must be adhered to at all times.

- Paper forms containing cardholder data must be sent through a mail courier in a locked bag.
- Credit cards left overnight must be stored in the secure vault locked in a safety cabinet.
- Credit card information should never be left unattended on a desk, computer, or machine. If an authorized person needs to leave their desk for any reason, all cardholder data must be securely locked in a safe.
- Only authorized processors will have access to cardholder data for processing gift transactions.
- Paper copies containing cardholder data will be destroyed after it has been processed at which point they will be cross-cut shredded.
- Credit card information must not be copied, faxed, emailed, or sent through campus mail.
- The best way to communicate credit card information is over the phone. Do not leave a voicemail containing cardholder data.
- Cardholder data should never be saved or stored on a computer.
- Never process a credit card through a desk computer. All credit cards processed on a computer must be done on the secured VDI terminal.
- When imaging gift documentation for credit card transactions, redact all but the last four digits of the credit number and redact the security code.