Augsburg College
Credit Card Policies for storing, processing & transmitting cardholder data

Latest Update: 12-27-10
Organizational Contacts: Staney Rostad, Controller, x1210 and Bradley Christ, Director of IT x1345

Background:

Our contracted merchant account provider - Wells Fargo, has required us to comply with certain best practices around accepting and processing credit card payments, referred to as PCI standards. The standards are designed to protect cardholder data and an overview of PCI requirements is as follows:

"PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all organizations that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc."

Augsburg Policy:

Consistent with PCI standards, Augsburg College's credit card policies consist of the following:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors.

Key practices of the Augsburg credit card policy:

1. Do not store account numbers or other sensitive authentication data after authorization – all paper with credit card numbers must be permanently masked or destroyed
2. Do not display the entire card number on receipts and records
3. Only personnel trained to observe the Augsburg credit card policies should have authority to processes credit card transactions
4. Access to all terminals and computers that process credit card transactions will be strictly controlled
5. In the event of a compromise of customer credit card numbers, notify the Augsburg Controller immediately, who will in turn contact the appropriate law enforcement agency, the merchant bank and the various credit card associations.