AUBURN UNIVERSITY AND AFFILIATED ORGANIZATIONS
POLICIES FOR CREDIT CARD PROCESSING AND SECURITY

1.0 Credit Card Acceptance and Processing

In the course of doing business at Auburn University, including Auburn University at Montgomery, and affiliated organizations, it may be necessary for a department or other unit to accept credit cards for payment. The opening of a new merchant account for the purpose of accepting and processing credit cards at the University is done on a case by case basis. Any fees associated with the acceptance of the credit card in that unit, will be charged to the unit.

1.1 Interested departments or units should contact the Electronic Payment Coordinator to begin the process of accepting credit cards.[1] Steps include:

1. Completion of an “Application to become a Merchant Department”.
2. Completion of training.
3. Read and sign-off on the University’s “Policies for Credit Card Processing and Security”, including ensuring ongoing compliance with all requirements of the policy.
4. If applicable, submit application for E-commerce for approval by the E-commerce committee. The application and policy are found at http://www.auburn.edu/oit/it_policies/ecommerce_management.php.

1.2 Any department accepting credit cards on behalf of the University or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions. This individual is referred to as the Merchant Department Responsible Person or MDRP. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDRP is unavailable.

1.3 Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Office of Cash Management or Student Financial Services.

1.4 Annual reviews will be done with each department to discuss updates and any environmental changes with credit cards due to security threats if any, and protection methods evolving rapidly throughout the year.

[1] In the event there is no individual in this role formally at Auburn University, then the Electronic Payment Coordinator will be the person performing the function of such role as part of assigned responsibilities.

2.0 Credit Card Data Security Policy

This policy addresses Payment Card Industry (PCI) Data Security Standard (DSS) that are contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment.[2] The policy covers the following specific areas contained in the PCI standards related to cardholder data: Collecting, processing, transmitting, storing and disposing of cardholder data.

Procedures must be documented by authorized departments and be available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

2.1 Cardholder data collected are restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access and review the list monthly to ensure that the list reflects the most current access needed and granted.
2.2 Cardholder data, whether collected on paper or electronically, are protected against unauthorized access.
2.3. All equipment used to collect data is secured against unauthorized use in accordance with the PCI Data Security Standard.
2.4 Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data.
2.5 The Office of Information Technology is responsible for PCI compliance for the electronic payment gateway (currently Touchnet) and all other centrally administered servers that process, store or transmit cardholder data. Individual departments are held responsible for PCI compliance for all departmental procedures, applications, point of sale devices and departmentally administered servers that process, store or transmit cardholder data. Additionally, these procedures, applications and systems should comply with Office of Information Technology policies, E-Commerce Policy and any applicable distributed information technology unit standards. All controls, including firewalls and encryption, should be documented and verified.
2.6 Email should not be used to transmit credit card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined in #2.10 below is critical.
2.7 If a fax machine is regularly used to transmit credit card information to a merchant department, that machine should be a stand alone machine with appropriate physical security. Disposal of credit card information provided via fax should follow #2.10 below.
2.8 No database, electronic file, or other electronic repository of information will store credit/debit card numbers, the full contents of any track from the magnetic stripe, or the card-validation code.
2.9 Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.

2.10 Cardholder data should be retained for three months after the end of the fiscal year in which the records were created, but must be deleted or destroyed immediately following the required retention period. The maximum period of time the data may be retained is 15 months. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the record retention requirements. Paper documents should be shredded in a cross-cut shredder. Before disposal or repurposing, computer drives should be sanitized in accordance with the University's Electronic Data Disposal Policy.

Departments should ensure that Auburn University Purchasing Card data are protected in a similar manner and institute the above components, particularly as it relates to storage and disposal of cardholder data.

3.0 Responding to a Security Breach

In the event of a breach or suspected breach of security, the department or unit must immediately execute each of the relevant steps below:

3.1 Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available.
3.2 Disconnect the computer/devices(s) from the network. To disconnect the device from the network, simply unplug the Ethernet (network) cable, or if the computer uses a wireless connection, disconnect from the wireless network.
3.3 DO NOT turn the computer device off or reboot. Leave the device powered on and disconnected from the network.
3.4 Notify the Electronic Payments Coordinator (Office of Cash Management) and the dean, director or department head of the unit experiencing the breach. Email (from an unaffected system) may be used for initial contact but the details of the breach should not be disclosed in email correspondence.
3.5 Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on to the machine and/or change passwords; do not run a virus scan). In short, leave the system(s) alone, disconnected from the network, and wait to hear from a security consultant.

If warranted, the Credit Card Manager will alert the merchant bank, the payment card associations, Internal Audit, General Counsel, and the Executive Vice President A suspected breach may be reported to Auburn University by the processing bank or an outside party. In that case, the Office of Cash Management will notify the campus merchant involved in the suspected breach and the relevant steps outlined in 3.0 above should be executed. A detailed incident response plan will be maintained by Office of Cash Management.

4.0 Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments which may be imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

5.0 Other Related Policies and Forms

E-Commerce Management - http://www.auburn.edu/oit/it_policies/ecommerce_management.php
Collections, Contributions and Accounts Receivable -
http://www.auburn.edu/administration/business_office/policy_manual/collect.html
Data Security-
http://www.auburn.edu/oit/it_policies/data_security_policy.php
Electronic Data Disposal Policy -
https://fp.auburn.edu/gradschl/public_html/Policies/Electronic_Data_Disposal.pdf
Payment Card Industry Data Security Standards –
https://www.pcisecuritystandards.org

6.0 Definitions

Cardholder data –_Any personally-identifiable data associated with a cardholder. Such data include account number, expiration date, name, address, social security number, Card Validation Code, Card Verification Value, Card Identification Number, or Card member ID.

Merchant Department – any department or unit (can be a group of departments or a subset of a department) which has been approved by Auburn University to accept credit cards and has been assigned a Merchant identification number.

Merchant Department Responsible Person (MDRP)_– an individual within the department who has primary authority and responsibility within that department for credit card transactions.

PCI-DSS -_Payment Card Industry Data Security Standards

TouchNet Gateway_– the only approved gateway for processing credit card transactions per the University's E-Commerce Management policy.