Policy Title:	Payment Card Industry Data Standard Security (PCI DSS) Policy
Policy Number:	UNIV-480
Revision Date:	March 2021
Policies Superseded:	None
Policy Management Area(s):	Information Technology Services Finance and Administration

SUMMARY:

Coastal Carolina University is committed to protecting and preserving the privacy and security of payment card data while conducting University business operations. The focus of the Payment Card Industry Data Standard Security (PCI DSS) policy is to protect against payment card fraud in e-commerce and terminal-based transactions. This policy defines and provides requirements and guidance for all payment card activities and establishes required practices for all members of Coastal Carolina University. This policy adheres to and is in compliance with the credit card industry's Payment Card Industry Data Security Standards as set by the PCI Security Standards Council. The policy deals with access to Coastal Carolina University's computing and network resources with regard to payment card processing as well as any freestanding payment card processing unit or point-of-sale system.

Coastal Carolina University does not store credit card information.

POLICY:

I. DEFINITIONS

A. Cardholder: person/agency to whom a card is issued or any individual authorized to use a card.

B. Cardholder data: full magnetic stripe or the Primary Account Number (PAN) plus any of the following:

1. cardholder name
2. expiration date
3. service code
4. CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card

5. other Personally Identifiable Information (PII) stored on the card

C. Credit card processing: act of storing, processing, or transmitting credit card data.

D. E-commerce application: any network-enabled financial transaction application.

E. ISO 27002: The International Standards Organization document defining computer security standards.

F. Merchant: University unit that accepts Visa, MasterCard, American Express or Discover payment cards using the University's merchant processor(s). A merchant is assigned a merchant identification number (MID) by the Office of Student Accounts.

G. Payment Card: includes credit and debit cards bearing the logo of Visa, MasterCard, American Express or Discover used to make a payment.

H. Payment Card Industry Data Security Standard (PCI DSS): PCI DSS is a standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customers' credit card data. The standard was developed by the PCI Security Standards Council to increase control of cardholder data to reduce payment card fraud and exposure.

   1. The Council Founding members are Visa, MasterCard, Discover, American Express and the Japanese Credit Bureau (JCB).

I. POS device: point-of-sale (POS) computer or payment card terminals, either running as stand-alone systems or connecting to a server, that are ordered by the Office of Student Accounts and approved by Information Technology Services (ITS).

J. Restricted data: any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protections whether in storage or in transit.

K. Virtual payment terminal: web-browser-based access to a third-party service provider website to authorize payment card transactions when the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card.

I. Web development: the design, development, implementation and management of the user interface of the e-commerce application.

II. APPLICABILITY AND SCOPE

A. The PCI DSS policy applies to:

1. All departments, employees, student workers and organizations of Coastal Carolina University who accept and transmit payment card information to conduct University business.
2. All external organizations contracted by University departments, affiliates or employees to provide goods or services on behalf of Coastal Carolina University. Contracts should contain terms that are consistent with this policy and must be approved by University Counsel, ITS and the Office of Financial Services **prior** to the execution of the contract.
3. All departments, affiliates, employees and student workers of Coastal Carolina University who utilize payment card services from third parties.

B. Requirements for merchant departments using a payment card terminal, as well as merchants processing or transmitting transactions using e-commerce, are as follows:

1. Terminal transactions include face-to-face transactions using a network connection, a phone line (where necessary) or cellular terminals. In some cases, a terminal's keypad may be used to enter card-not-present transactions where cardholder data was received via postal mail or over the phone.
2. E-commerce transactions include the following:
   a. links on University websites redirecting individuals to another payment website;
   b. IP-connected terminals processing payments on the Internet;
   c. point-of-sale transactions at a computer cash register using PCI payment applications, including point-of-sale software on a computer, to transmit, process or store cardholder data;
   d. use of third-party vendor's virtual payment terminal to transmit cardholder data; and
   e. transactions transmitted on the University network.

III. POLICY

A. Payment card processing approval and management

1. All requests for access to credit card acceptance must be made to the Office of Financial Services and to ITS.
2. All Coastal Carolina University divisions and departments desiring to accept payment for financial transactions by POS and/or electronically via the Internet using e-commerce are required to process all transactions through gateways approved by the Office of Financial Services and by ITS. The Application for New Payment Card Merchants must be completed and approved in advance of any implementation or third party contract.
3. The University Controller and the Chief Information and Technology Officer, or named designees, in coordination with Procurement Services and the University Counsel, must approve all requests to begin accepting payment cards at Coastal Carolina University before a unit enters into any contract or purchase of software and/or equipment. This requirement applies regardless of the transaction method used (e.g., e-commerce, POS

device or e-commerce outsourced to a third party). Approved units must register their payment card processing information with the Office of Financial Services and with ITS.

4. All technology implementations (including approval of authorized payment gateways) associated with the payment card processing must be in accordance with the PCI DSS Policy and be approved by ITS and by Procurement Servicers prior to entering into any contract or purchasing software and/or equipment.
5. The University provides secure and PCI-compliant transactions through SC.GOV, Fiserv (formerly First Data/Sun Trust) and ACI Worldwide (other vendors may be approved following procurement procedures and approval channels). For more information, please contact the Office of Financial Services or ITS.
6. Products or services provided by e-commerce sites are limited to those that support the Coastal Carolina University mission.
7. Tasks including, but not limited to, faxing, e-mailing, and scanning payment forms; maintaining spreadsheets, receipts or documents in electronic form; and using messaging technology are prohibited if they include cardholder data.
8. Cardholder data must not be stored in any way on the Coastal Carolina University computers or networks. Credit card numbers should never be written down or appear in emails.
9. Third-party vendors must have an online privacy policy that is easily located by the potential customer who visits their websites. The privacy policy must clearly state the limitations of use, rules regarding retention and protection measures related to data that customers submit. It should also state what, if any, electronic monitoring and HTTP cookie use CCU intends to perform with a visitor's electronic connection. The site must also provide contact information for customers to ask questions about the privacy policy. Terms and agreements between third-party vendors and the University must address the protection of cardholder data in adherence with the law, University policies and PCI DSS standards.

B. Payment card maintenance standards and responsibilities

1. All members of the University community share the responsibility for protecting the information and data with which they are entrusted.
2. All cardholder data should be classified as restricted.
3. The Office of Financial Services, ITS and all other departments that manage payment card transactions must adhere to the strict requirements of this policy and of the industry PCI DSS standards.
4. Access to payment card processing systems and related information must be restricted to appropriate personnel. In some cases, personnel may be subject to background and credit checks prior to participating in the processing of credit card payments. All employees and student workers involved in e-commerce or POS transactions must understand, complete annual training, and attest to all requirements as outlined in this PCI DSS Policy and the Payment Card Procedures v3.2 prior to handling payment transactions. ITS and the Office of Financial Services must be provided with a list of all individuals by merchant department handling payment card transactions on an ongoing basis.
5. All individuals who handle, transmit, support or manage payment card transactions received by the University must complete the University PCI training upon hire and

annually thereafter. PCI overview training modules are coordinated by the Office of Financial Services.

6. All servers and POS devices will be administered in accordance with the University's requirements of the PCI DSS standards.
7. POS devices with point-to-point encryption (P2PE) protection should be used where available and compatible with software systems.
8. ITS must maintain and enforce secure network infrastructure University wide in accordance with the requirements of the PCI DSS standards and with legal, policy and industry standard best practice requirements.
9. ITS and the Office of Financial Services must promptly inform current and potential merchants of any changes to applicable policies, laws, regulations and industry standards.
10. Each department responsible for payment card processing will be subject to an Annual Self-Assessment Questionnaire and a Quarterly Network Scan as scheduled by ITS-Information Security. All systems processing cardholder data must comply with the PCI DSS Policy and the associated requirements. ITS and the Office of Financial Services will assist in the initial self-assessment. To combat the loss of payment card information, e-commerce sites must comply with all security requirements as outlined in the PCI-DSS standards.
11. Third-party source code (HTML, CGI or script) should be provided to ITS-Information Security upon request.
12. Third parties providing payment gateways or who interact in any way with payment cards as a form of payment must provide Attestation of Certification (AOC) of PCI-DSS compliance annually.
13. Coastal Carolina University reserves the right to request that third-party vendors provide evidence of adequate liability insurance for data breach.
14. Only approved Coastal Carolina University logos may be used on e-commerce sites associated with the University.

C. Reporting Security Incidents

1. Protecting data is everyone's responsibility. Known, suspected and alleged incidents involving lost, disclosed, stolen, compromised or misused cardholder data must be reported immediately to the following individuals.
   a. The University Controller and
      (1) a designated individual in the Office of Financial Services.
         (a) The designated individual in the Office of Financial Services must report any such incident immediately to the office of the Chief Information and Technology Officer and by e-mail to issecurity@coastal.edu.
   b. Security incident reports must not disclose cardholder data.

D. Compliance

1. Failure to comply with the PCI DSS Policy and the above-referenced requirements will be deemed a violation of University policy and may result in suspension of electronic payment capability for the affected department.
2. It is the responsibility of all individuals to whom this policy applies to be informed of and follow the requirements under this policy and any associated documents to protect cardholder data.
3. Employees who violate this policy may be subject to disciplinary action, including but not limited to, termination of employment and/or potential criminal prosecution under applicable federal, state and local laws.
4. Other individuals to whom this policy applies who violate this policy are subject to appropriate sanctions, including but not limited to, termination of the relationship and/or potential criminal prosecution under applicable federal, state and local laws.
5. Technology that does not comply with the PCI-DSS standards will be disconnected from network services.