21.01.02.R0.02 Credit Card Information Receipt, Custody, and Security Procedures

Approved September 15, 2008
Revised March 31, 2014
Next Scheduled Review March 31, 2019

Procedure Statement

The purpose of this procedure is to identify the process that must be followed when processing credit card information and to identify the necessary controls to protect the information being processed.

Reason for Procedure

System Regulation *21.0102 Receipt, Custody and Deposit of Revenues* require members to adhere to industry security standards to protect cardholder date. Members must complete the payment card industry data security training.

Procedures and Responsibilities

1. ON-LINE PROCESSING

   All on-line payments and sales using credit card verification and processing shall be handled through LeoPay, TouchNet, Global Payment and other systems established by Financial Services and approved through the Chief Information Officer.

2. GENERAL PROCESSING CONTROLS

   2.1. Protection of Stored Data

      2.1.1. Sensitive cardholder data that includes account number, magnetic stripe data, card-validation code and expiration date must be properly disposed of when no longer needed. (See section 3.2.5. below)

      2.1.2. The full contents of any track from the magnetic stripe shall not be stored in agency and/or division databases, log files, or point-of-sale-products.

2.1.3. The card-validation code (three digits printed on the signature panel of a card) shall not be stored in university and/or department databases, log files, or point-of-sale products.

2.1.4. Account numbers must be stored securely in databases, logs, files, and backup media (for example, by means of encryption or truncation).

2.2. Access to Cardholder Data

2.2.1. Access to all cardholder data shall be restricted to employees with a legitimate need-to-know.

2.2.2. Written procedures regarding multiple security controls shall be developed and be in place to prevent unauthorized individuals from gaining access to the facilities and equipment, such as servers, workstations, laptops, and hard drives and media, containing cardholder data. Controls such as using cameras for sensitive areas, using badges that expire, physically escorting visitors in sensitive areas, or using visitor logs to retain an audit trail can be used. The procedures shall be developed under the responsibility of the division head or equivalent and approved by the Chief Information Officer. Written procedures shall be review concurrently with this procedure.

2.2.3. Cardholder data printed on paper or received by fax must be physically protected against unauthorized access such as by maintaining it in a locked area or shredding.

2.2.4. Written procedures shall be developed and be in place to handle secure distribution and disposal of backup and other electronic media containing sensitive cardholder data. They should include controls such as labeling media as confidential, sending media via secure couriers, or using secure disposal methods that will provide that assurance that sensitive data cannot be recovered. The procedures shall be developed under the responsibility of the department head or equivalent and approved by the Chief Information Officer. Written procedures shall be review concurrently with this procedure.

2.2.5. Cardholder data must be destroyed or deleted before the paper or electronic media is physically disposed of using methods such as shredding or sanitization.

2.3. Information Security Policies

2.3.1. Criminal history checks are conducted for new university staff. Periodic background checks may be performed for employees with access to cardholder data.

2.3.2. All third parties with access to sensitive cardholder data must be contractually obligated to comply with card association security standards. Please check the

PCI Security Standards Council for the latest version at: https://www.pcisecuritystandards.org/.

3. RESPONSIBILITIES

The department head or their equivalent for each area collecting and using credit card information is assigned the responsibility of ensuring that the above procedures are implemented in their respective areas.

Related Statutes, Policies, or Requirements

System Policy *21.01 Financial Policies, Systems and Procedures*

System Regulation *21.01.02 Receipt, Custody, and Deposit of Revenues*

University Procedure *21.01.02 R0.01 Credit Card Collection*

University Procedure *29.01.03.R0.02 Electronic Information Security*

University Procedure *29.01.99.R0.02 Information Technology Risk Assessment*

Contact Office

Office of Chief Information Officer
903.886.5421