512 POLICY - Payment Card Industry Security Standards

512.1 Statement of Policy

It is the policy of Redlands Community College to comply with applicable security standards and procedures in connection with its acceptance of various electronic payment transactions. The credit card industry (Visa, MasterCard, etc.) requires any organization or merchant that transmits, stores, or processes cardholders' information to comply with the security standards set by the Payment Card Industry Security Standards Council. An organization or merchant must be certified to be in compliance with the Payment Card Industry security standards in order to accept payments by credit cards. Redlands Community College will comply with those security standards.

512.2 Implementation and Compliance

The Redlands Community College Department of Technology is responsible for implementation of the Payment Card Industry security standards within Redlands Community College, for ongoing compliance with those standards, and for obtaining the necessary certifications of compliance.

512.3 Related Procedure

The Procedures section of the Policies and Procedures Manual contains a procedure related to this policy.

Adopted December 2010

512 PROCEDURE - Payment Card Industry (PCI)

512.1:1 Statement of Procedure

The Payment Card Industry Security Standards Council sets technical and operational standards that apply to organizations and merchants that store, process or transmit cardholder data. In order to accept credit card payments, Redlands Community College complies with those standards.

512.2:1 Implementation and Compliance

The Redlands Community College Department of Technology is responsible for implementing the security standards and procedures that are issued by the Payment Card Industry ("PCI") Security Standards Council. The Redlands Community College Department of Technology is also responsible for monitoring compliance with those standards and obtaining the required certifications of compliance. This includes the completion of an annual questionnaire provided by the PCI Security Standards Council which provides a means for assessing compliance. All Redlands Community College departments that accept credit cards as payment for products and services shall comply with the security standards and will be required to pass an audit of their internal systems and processes.

512.3:1 Specific Standards and Procedures

The Redlands Community College Department of Technology will develop, issue and implement appropriate security standards and procedures for compliance with the PCI security standards. The technical details of those standards and procedures may be obtained from the Redlands Community College Department of Technology. Among those standards and procedures are the following:

Data Retention. All credit card data processed shall be encrypted, and if stored, kept on a server with no outward-facing ports. Receipts shall be required to have all but the last 4 digits masked.

Document Disposition. Credit card information taken over the telephone or provided in any written form shall be shredded immediately after the credit card transaction is completed.

System Updates. Updates to the information technology systems that are associated with or involved in credit card transactions are not allowed until approved by the Redlands Community College Department of Technology. Only the Department of Technology is authorized to adjust configuration settings, to remove software or to install updates or patches, including security patches.

Security Patch Management. Security Patch Management is a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. Consequently, all system components directly associated with the cardholder data environment shall be securely hardened and configured with all necessary and appropriate patches and system updates for preventing the exploitation or disruption of mission-critical services. Additionally, all technology resources not directly associated with the cardholder data environment shall also be securely hardened and configured with all necessary and appropriate patches and system updates in order to prevent the exploitation or disruption of mission-critical services.

The Redlands Community College Department of Technology is responsible for security patch management. In accordance with best practices for Security Patch Management, the subsequent three (3) security concerns shall be highlighted throughout the Security Patch Management process. They are as follows:

- Vulnerability Identification. Identifying vulnerabilities consisting of a software flaw or a misconfiguration that may result in weakness in the security of a system within the system components directly associated with the cardholder data environment or any other I.T. resources
- Remediation. Determining and implementing the most appropriate remediation from among the three (3) primary methods: (1) installation of a software patch, (2) adjustment of a configuration setting and/or (3) removal of affected software.
- Threats. Anticipating, recognizing and responding to threats which are capabilities or methods of attack developed to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses and Trojan horses.

Adopted December 2010