Reynolds COMMUNITY COLLEGE

Policies and Procedures

TITLE: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

POLICY NO: 4-41 **EFFECTIVE DATE: 04/16/13**

VCCS POLICY NO: N/A **REVISED DATE: 10/25/18**

I. Purpose:

To provide policy for processing, transmitting, storing, and disposing of credit cardholder data that ensures the safety and confidentiality of cardholder information according to Payment Card Industry Data Security Standard (PCI DSS); to outline the authentication and access control requirements when accessing sensitive card data.

II. Definitions:

Cardholder data (CHD): those elements of credit card information which are required to be protected, including the Primary Account Number (PAN) in conjunction with cardholder name, expiration date, service code, and DVV/CVV2/CSC2.

Disposal: a manner of disposing cardholder data that renders all data unrecoverable, including paper documents and any electronic media, such as computers, hard drives, magnetic tapes, USB storage devices, and any other device that may capture and retain any CHD information.

Merchant department: any department or unit (can be a group of departments or a subset of a department) at J. Sargeant Reynolds Community College (Reynolds) which has been approved by the Virginia Community College System (VCCS) 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.

Payment Card Industry Data Security Standard (PCI DSS): the security requirements defined by the Payment Card Industry Security Standards Council and the five major credit card brands: Visa, MasterCard, American Express, Discover, and JCB.

III. Policy:

Payment Card Industry Data Security Standard (PCI DSS) is contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment in order to ensure the safety and confidentiality of cardholder information. PCI DSS standards are set by the PCI Security Standards Council and incorporated into the VCCS Information Standard. The VCCS Information Security Standard 18.2 – Compliance, includes the requirement under 18.2.4 –

Payment Card Industry Compliance, regarding the obligations of the VCCS and colleges that handle any cardholder data. Under the standard Reynolds is required to continually comply with PCI DSS, complete the appropriate Self-Assessment Questionnaire (SAQ) annually, and submit the SAQ to the acquiring bank.

IV. Procedures:

Specific operational steps, responsibilities, and guidelines, where applicable, will be contained in the companion document entitled Standard Operating Procedure: PCI Management.

V. Other Information:

Questions regarding the application of this policy and procedures should be directed to the vice president of finance and administration, and/or the primary information security officer.

PCI Document Library

PCI Security Standards Council Website

JSRCC Standard Operating Procedure: PCI Management