Columbus State University

Policy Name:	Payment Card Industry Data Security Standard Compliance Policy
Policy Owner:	Tom Helton
Responsible University Office:	Office of Business and Finance
Effective Date:	November 6, 2018
Policy Number:	TBD
Related Policies:	

I. Purpose

The purpose of Payment Card Industry Data Security Standard Policy (PCI DSS) is to prevent credit card fraud, hacking, and various other security vulnerabilities and threats, and to minimize the possibility of a breach of account data by adhering to the PCI DSS.

I. Policy Statement

Columbus State University shall be compliant with the current version of the PCI DSS at all times. All card handling activities and related technologies must comply with the PCI DSS in its entirety. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI DSS.

This policy will be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

II. Applicability

This policy applies to the following:

1. All personnel who store, process, transmit, have access to, or affect the security of account data, including all CSU faculty, staff, contractors, and students;

2. Any CSU employee who contracts with a third party vendor to handle and/or process account data***;*** and

All vendors, contractors, and business partners who store, process, transmit, have access to, or affect the security of account data on behalf of ***CSU. CSU c***ontracts shall require such vendors, contractors and business partners to be compliant with the PCI

DSS.

III. Training

All CSU personnel in positions that store, process, transmit, have access to, or affect the security of account data shall complete PCI DSS training upon hire and at least annually, and further, shall acknowledge, in writing or electronically, that they have read, understand and will comply with this Policy.