Payment Card Industry Compliance Policy

Approved By: Northeastern State University Policy Committee **Responsible Official:** Business Affairs (918) 444-2160	**History:** Adopted – July 25, 2017 **Related Policies:** E-Commerce **Additional References: Forms:**

PURPOSE

This policy ensures Payment Card Industry (PCI) compliance by all credit card merchants on the Northeastern State University campuses with national standards.

DISCLOSURE STATEMENT

Standards for PCI compliance are set by the PCI Data Security Standards (DSS) Board. Failure to comply with these standards may result in fines and/or the loss of the privilege of taking credit cards as a form of payment across the Northeastern State University campuses.

SPECIAL WORDING

eCommerce

Business transactions over electronic means including the internet and other means for electronic interactions such as automated phone banks, touch screen kiosks, or even ATMs.
Transactions can include debit/credit cards as well as electronic transfer of funds via ACH.

PCI

Payment Card Industry

Payment Card Industry Data Security Standard [PCI DSS]

Payment Card Industry Data Security Standard – a proprietary information security standard for organizations that handle branded credit cards including Visa, MasterCard, American Express, Discover, and JCB. The requirements include network, security (physical/logical), and monitoring components, among others.

POLICY

Northeastern State University adheres to all PCI requirements to ensure the safety and integrity of all eCommerce transactions conducted under NSU's authority.

NSU will enforce PCI DDS compliance by all departments using eCommerce to perform business activities.

Bursar Services has the authority to enforce compliance.

PROCEDURE(S)

As the responsible authority over eCommerce and the devices used to effect eCommerce, Bursar Services is responsible for the following:

A. Maintaining a list of all credit card devices including their location and serial numbers.
B. Ensuring all devices and Ethernet lines are inspected regularly for tampering or replacement.
C. Establishing a mandatory training program for employees who work with eCommerce devices.
D. Conducting training to include how to check equipment and lines for tampering or replacement. If storage of cardholder data becomes necessary, training must include proper storage measures and how to destroy cardholder data when no longer needed.
E. Maintaining a list of service providers with descriptions of services provided.
F. Monitoring the PCI DSS compliancy of all service providers by requesting a copy of their PCI Compliancy documents yearly.