



41.209: Electronic Commerce

Responsible Executive: Vice President for Finance and Business
Responsible Office: Controller
Related Policy: 60.201; 61.001; 61.002
Approved-On Date: January 11, 2006
Effective Date: January 11, 2006
Revision Date:

Policy

Norfolk State University will engage in and actively promote electronic commerce, (E-Commerce), which is regarded as a highly effective and efficient way to perform sales related business activities. However, reasonable steps will be taken to protect the personal information and privacy of purchasers. Furthermore, it is in the best interest of the University to automatically transfer E-Commerce transaction data directly into University internal financial systems when this is technologically feasible.

Purpose

The purpose of this policy is to provide guidance on procedures to follow that will help ensure E-Commerce based business at NSU is conducted in a safe and secure manner to minimize risk to both the University and the customers.

Procedures

I. Definition

E-Commerce is defined, for the purpose of this policy, as the buying and selling of goods and services on the Internet, primarily the World Wide Web. Generally, this means the University sells its goods and services to individual buyers. This policy does not address other forms of electronic commerce such as “business-to-business” sales and ordering performed via similar electronic means and conducted between the University and businesses as well as other public and/or private institutions.

II. Relation to University Mission

The use of electronic commerce at the University must be consistent with University Policy 60.201 which specifies that the use of technological resources must be for official business.

III. Authorized Vendors

Norfolk State University will contract with one or more reputable Internet commerce services vendors to handle the authorization and management of electronic orders. Vendors selected must meet University requirements for security and any systems integration needed. These arrangements will allow the University to:

1. Consistently require the vendor to take necessary and reasonable steps to ensure that transactions are secure.
2. Ensure appropriate integration with University financial systems.
3. Ensure that parties comply with University policies on the use of names and the privacy of individuals.
4. Use tested emergency response and recovery procedures.
5. Leverage University transactions to reduce costs.
6. Provide current technology and support for applications development.

IV. Confidentiality of Data

Complete credit card details are said to be “in transit” on the University network and are not permanently stored on the web or database servers at any stage of the transaction processing. Once the transaction has been processed, credit card details are no longer known to any of the University systems.

NSU systems may retain transaction tracking data that may include the last four digits of a customer’s credit card number which can be used for transaction tracking, processing, and verification.

The University will not send electronic mail messages to E-Commerce customers asking them to update their credit card or bank information. If anyone receives such a request, they should not reply and they should forward the message to the Office of Information Technology Help Desk (helpdesk@nsu.edu) immediately so the incident can be promptly investigated.

Departments/activities of the University engaging in E-Commerce must:

1. Safeguard the confidentiality of data relating to the purchases of goods or services, and, retain essential data in accordance with the records retention schedule established by the Library of Virginia.
2. Use only secure connections to University approved transaction processing service vendors.

3. Maintain information in a secure manner and restrict access to only those personnel who have a valid need to know.
4. Adhere to University privacy guidelines and security procedures, and, establish links to the guidelines at each point-of-sale. If it is felt that a valid business requirement mandates a departure from the privacy guidelines, the department/activity must then consult with the Associate Vice President for Technology.