1. **Purpose.** The purpose of this policy is to assist the University System of New Hampshire (USNH) and its institutions in complying with the Payment Card Industry Data Security Standard (PCI DSS). This policy addresses the standards that are contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment. The policy covers the following specific areas contained in the PCI standards related to cardholder data: Processing, transmitting, storing and disposing of Card Holder Data (defined below).

2. **Scope.** These policies apply to all USNH employees, systems and networks involved with credit card handling which includes transmission, storage and/or processing of credit card numbers at USNH.

3. **Authority.**

   a. The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and Japanese Credit Bureau. These security requirements apply to all transactions surrounding the payment card industry. Electronic and paper handling are covered by this standard. The requirements apply to any organization involved with handling cardholder data. There is an annual reporting requirement that must be completed by the holder of the merchant ID. Further details about this reporting requirement can be found at the PCI Security Standards Council Web site ([https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)).

   b. USNH requires that all campus organizations and departments collecting credit card receipts:

      i. Follow the USNH PCI DSS administrative and technical policies;

      ii. Develop pertinent local practices, procedures and documentation to ensure compliance with PCI standards; and,

      iii. Provide training for the employees and others that handle Card Holder Data as defined below.

4. **Revision.** These policies may be updated at anytime and must be reviewed annually by designated merchants, administrators and staff for changes.

5. **Definitions.**

   a. **Payment Card Industry Data Security Standards (PCI-DSS) -** The security requirements as defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands:

      i. Visa
      ii. MasterCard
iii. American Express  
iv. Discover  
v. Japanese Credit Bureau (JCB)

b. Card Holder Data (CHD) – Those elements of credit card information that are required to be protected when stored? These elements include the Primary Account Number (PAN) in conjunction with:

i. Cardholder name  
ii. Expiration Date  
iii. Service code  
iv. CVV/CVV2/CSC2

c. Merchant Department – Any department or unit (can be a group of departments or a subset of a department) which has been approved by the USNH to accept credit cards and has been assigned a Merchant identification number.

d. Merchant Department Responsible Person (MDRP) – An individual within the department who has primary authority and responsibility within that department for credit card transactions.

6. Credit Card Acceptance and Handling.

a. In the course of doing business at any USNH institution or organization including USNH-affiliated organizations, it may be necessary for a department or other unit to accept credit cards for payment. The opening of a new merchant account for the purpose of accepting and processing credit cards is done on a case-by-case basis. Any fees associated with the acceptance of the credit card in that unit, will be charged to the unit.

b. Interested departments or units should contact their respective institutional financial administration to begin the process of accepting credit cards. Steps include:\1

i. Completion of cost-benefit analysis showing net cost savings or additional revenues to be achieved by collecting revenues via credit cards  
ii. Completion of an “Application to become a Merchant Department”  
iii. Completion of training  
iv. Read and sign-off on the “Policies for Credit Card Processing and Security”, including ensuring ongoing compliance with all requirements of the policy  
v. If applicable, submit application for E-commerce for approval by the E-commerce committee.  
vi. Once campus financial administration has approved the request it should be forwarded to USNH Accounting Services for coordination of setup requirements with the merchant bank.

c. Any department accepting credit cards on behalf of the institution or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions. This individual is referred to as the Merchant Department Responsible Person or MDRP. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDRP is unavailable.
d. Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the USNH System Office.

7. **Credit Card Data Security Procedures.** Procedures must be documented by authorized departments and be available for periodic review. Departments must have the following components in their procedures and ensure that these components are maintained on an ongoing basis.

a. Access to CHD must be restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access and review the list monthly to ensure that the list reflects the most current access needed and granted.

b. CHD, whether collected on paper or electronically, must be protected against unauthorized access.

c. All equipment used to collect CHD must be secured against unauthorized use or tampering in accordance with the PCI Data Security Standards.

d. Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or file cabinets that store the equipment, documents or electronic files containing CHD.

e. **Email** Any unencrypted electronic method such as email should not be used to transmit credit card or personal payment information, nor should it be accepted as a method to supply such information. In the event this does occur, disposal as outlined below is critical. Also see item 6.) in the Best Practices Guide for additional information in this regard.

f. Fax machines used to transmit credit card information to a merchant department must be stand alone machines (rather than multi-function/multi-user devices) with appropriate physical security.

g. No database, electronic files, or other electronic repositories of information may store the card-validation code or the full contents of any track from the magnetic stripe.

h. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.

i. CHD should not be retained any longer than the documented business need or required retention period after which, it must be immediately deleted or destroyed. The maximum period of time the data may be retained shall be set by the appropriate financial administration office of the affected institution, in consultation with the USNH System Office. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the record retention requirements.

**Disposal –** CHD must be disposed of in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices, (Before disposal or repurposing, computer drives should be sanitized in accordance with the USNH and applicable USNH Institution Electronic Data Disposal Policy). The approved disposal methods are:
Cross-cut shredding
   i. Incineration
   ii. Approved shredding or disposal service
   iii. All electronic media must be destroyed in a manner that renders it unrecoverable.

j. USNH Purchasing Card data shall be protected in a similar manner and institute the above components, particularly as it relates to storage and disposal of CHD.

k. Employee security lapses will be logged and resolved; lapses are defined as cases where employees did not follow correct procedure, but which did not result in a security breach.

Responding to a Security Breach. In the event of a breach or suspected breach of security, the department or unit must immediately execute each of the relevant steps outlined below in addition to following applicable local institutional or departmental incident management procedures:

a. Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation:
   i. Date and time
   ii. Action taken
   iii. Location
   iv. Person performing action
   v. Person performing documentation
   vi. All personnel involved

b. Contact the USNH IT Security Office and the institutional IT or Information Security office for proper direction of preservation of electronic data. The steps should include:
   i. Disconnect the computer/devices(s) from the network. To disconnect the device from the network, simply unplug the Ethernet (network) cable, or if the computer uses a wireless connection, disconnect from the wireless network.
   ii. DO NOT turn the computer device off or reboot. Leave the device powered on and disconnected from the network.

c. Notify the Electronic Payments Coordinator and the dean, director or department head of the unit experiencing the breach.

d. Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on to the machine and/or change passwords; do not run a virus scan). In short, leave the system(s) alone, disconnected from the network, and wait to hear from a security consultant.

e. If a suspected or confirmed intrusion / breach of a system has occurred, the MDRP will alert the merchant bank, the payment card associations, Internal Audit, General Counsel, and the Executive Vice President.

f. A suspected breach may be reported to USNH by the processing bank or an outside party. In that case, USNH will notify the campus merchant involved in the suspected breach and the relevant steps outlined in Section 8 above should be executed.
9. A detailed incident response plan will be maintained by USNH IT Security. This incident response plan shall be in accordance with the parameters set forth by the Card Brands.

10. Sanctions

a. Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments which may be imposed by the affected credit card company will be the responsibility of the impacted unit.

b. Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. USNH will carry out its responsibility to report such violations to the appropriate authorities.


a. CampusGuard provided a set of best practices for USNH to incorporate into merchant office procedures to better understand and comply with the requirements of the standard. All USNH organizations that are subject to the USNH PCI-DSS policies are expected to follow these best practices.

b. Where conflict may exist between local institutional practices and the CampusGuard recommended practices, the senior PCI DSS compliance representatives of the institution will consult with the USNH System Office about reasonable resolution of the conflict.

12. PCI DSS Information Technology (IT) Policy. Each USNH Institution will document PCI DSS Information Technology policies and procedures using, at minimum, the template provided by CampusGuard.

13. Employee Change Form For Merchant Location. Merchants will notify their institutional PCI DSS coordinator of any change of personnel involved in payment card processing. This includes any new hires or personnel who have been assigned new duties that include payment card processing and/or settlement duties. It also includes employees that have left their position and are no longer involved in payment card processing. Notification will consist of, at minimum, filling out the change form provided by the institutional PCI DSS coordinator.

14. Employee Statement of Understanding. Supervisors will ensure that employees who handle CHD as part of their employment or other activity at USNH fill out and sign the employee statement of understanding form provided by the institutional PCI DSS coordinator.

15. PCI DSS Annual Merchant Questionnaire. Each merchant will complete and/or update an annual compliance questionnaire as instructed by the USNH System Office.