1. **Purpose.** The purpose of this guideline is to assist the University of New Hampshire (UNH) in complying with the Payment Card Industry Data Security Standard (PCI DSS). This guideline addresses the standards that are contractually imposed on University merchants that accept payment cards as forms of payment and covers the following specific areas contained in the PCI DSS related to cardholder data: processing, transmitting, storing and disposing of Card Holder Data as defined below.

2. **Scope.** The guideline applies to all UNH departments, employees, systems and networks involved with payment card handling which includes transmission, storage and/or processing of payment card data on behalf of UNH.

3. **Authority.** The PCI DSS is a mandated set of requirements agreed upon by the five major payment card companies and maintained by the Payment Card Industry Security Standards Council (PCI SSC). Electronic and paper handling are covered by this standard and 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 information about the PCI DSS requirements and the reporting requirement can be found at the PCI SSC web site (https://www.pcisecuritystandards.org).

The UNH PCI Steering Committee (UNH PCI SC), under the authority of the Vice President of Finance and Operations (VPFA), is charged with monitoring and reporting on merchants' compliance to the standard. UNH requires that all organizations and departments accepting payment cards:
   a. Follow the UNH PCI DSS administrative and technical guidelines;
   b. Have in place pertinent local practices, procedures and documentation to ensure compliance with PCI standards; and,
   c. Provide training for the employees and others that handle Card Holder Data as defined below.

4. **Revision.** This guideline may be updated at any time and must be reviewed annually for changes by UNH merchants.

5. **Definitions.**
   a. Payment cards – any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard, or Visa, Inc including credit, debit, gift and reward cards. For purposes of this guideline, payments cards do not include UNH Cats Cache or ID cards.

   b. Payment Card Industry Data Security Standards (PCI DSS) - The security requirements as defined by the PCI SSC and the major Payment Card Brands.

   c. Card Holder Data (CHD) – Those elements of payment card information that are required to be protected. These elements include the Primary Account Number (PAN) or the PAN in conjunction with:
      i. Cardholder name
      ii. Expiration Date
      iii. Service code
      iv. CVV/CVV2/CSC2
d. Merchant – Any department or unit (can be a group of departments or a subset of a department) which has been approved by UNH to accept payment cards and has been assigned a Merchant Identification (MID) number.

e. Merchant Department Responsible Person (MDRP) – An individual within the department who has primary authority and responsibility within that department for payment card transactions and ensuring compliance with PCI DSS.

f. Service Provider: A business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity.

6. Payment Card Acceptance and Handling. In the course of doing business at UNH, it may be necessary for a department or other unit to accept payment cards for payments or to cease taking payment cards. Any fees associated with the acceptance of payment cards in that unit, will be charged to the unit. Prospective merchant departments or units must:

   a) contact their Business Service Center (BSC) Director or designee to begin the process of accepting credit cards
   b) read and sign-off on this document including ensuring ongoing compliance with all requirements of the guideline
   c) designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. This individual is referred to as the MDRP. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDRP is unavailable.

7. Payment 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 regularly to ensure that the list reflects the most current access needed and granted.
      i. All employees with access to CHD will have had a criminal background check before being allowed to access CHD
   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 DSS.
   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. Any unencrypted electronic communication method such as email shall not be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. In the event this does occur, disposal of the data as outlined below is critical. Each merchant department will include in the departmental PCI DSS guideline the proper method to handle and respond to emails or other insecure communications sent by customers containing CHD.
   f. Fax machines used to transmit payment card information to a merchant department must be stand-alone machines (rather than multi-function/multi-user devices) with appropriate physical security.
   g. No University database, electronic files, or other electronic repositories of information may store any CHD including the card-validation code or the full contents of any track from the magnetic stripe.
h. Portable electronic media devices shall not be used to store CHD. These devices include, but are not limited to, the following: laptops, tablet computers, compact disks, USB flash drives, smartphones and portable external hard drives.

i. CHD shall not be retained any longer than required to authorize the transaction, and must be immediately deleted or destroyed following authorization. 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. Access to stored CHD must be logged with the date and time of access, along with the identity of the employee accessing the secured data and customer contact information in the case of loss (to notify the customer).

j. Disposal – CHD must be disposed of in a manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices, (Before disposal or repurposing, computer drives shall be wiped in accordance with the USNH guideline). The approved disposal methods are:
   i. Cross-cut shredding
   ii. Incineration
   iii. Approved shredding or disposal service
   iv. Wiping and/or physical destruction of electronic media which renders the data unrecoverable.

k. Scanning for CHD: All work computers of employees authorized to handle CHD and shared workstations related to merchant operations will be scanned with the University authorized scanning tool on a regular basis to ensure no CHD is stored on those computers in case of accident, negligence, or other reasons. Scans will be conducted at least monthly.

l. 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.

m. 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.

8. **Service Provider Relationships.** Merchants and their service providers must have a defined and consistent level of understanding about their applicable PCI DSS responsibilities.

   a. UNH Merchants that utilize a service provider for payment transmission, processing, or storage must obtain a written agreement from the service provider stating that the named service provider is responsible for the protection and security of the cardholder data that the service provider possesses or otherwise stores, processes, or transmits on behalf of UNH.

   b. The written agreement must specify the PCI DSS requirements for which the service provider is responsible and those for which the UNH Merchant is responsible.

   c. Merchants should communicate to employees the PCI requirements for which the merchant is responsible.

9. **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 institutional or departmental incident management procedures:

   a. Disconnect the computer/devices(s) from the network. To disconnect the device from the network, unplug the Ethernet (network) cable, and/or if the computer uses a wireless connection, disconnect from the wireless network.

   b. DO NOT turn the computer or device off or reboot. Leave the device powered on and disconnected from the network.
c. 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.

d. Contact the UNH Information Security Services (ISS) office and departmental IT support for proper direction of preservation of electronic data.
   i. A detailed incident response plan will be maintained by UNH ISS. This incident response plan shall be in accordance with the parameters set forth by the Card Brands.

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

f. Notify the MDRP and the dean, director or department head of the unit experiencing the breach.

g. If a suspected or confirmed intrusion/breach of a system has occurred, the MDRP will alert the Office of the VPFA, USNH Internal Audit and the USNH General Counsel. Additional steps may be required.

h. The Office of the VPFA will coordinate external communications including but not limited to the merchant bank, USNH Treasury Operations or the news media, as may be required or applicable.

i. A suspected breach may be reported to UNH or USNH by the processing bank or an outside party. In that case, UNH or USNH will notify the campus merchant involved in the suspected breach and the relevant steps outlined above should be executed.

10. **Sanctions.** Failure to meet the requirements outlined in this guideline (e.g., non-compliance to PCI DSS) may result in termination of the ability to accept payment cards for the impacted merchant. Additionally, if appropriate, any fines and assessments which may be imposed by the affected payment card company and/or the bank will be the responsibility of the impacted merchant. University employees in violation of this guideline may also be subject to sanctions, as defined by the UNH Acceptable Use Policy (AUP).

Departmental sanctions process:

a. Non-compliant merchants will define and implement corrective action(s) to achieve PCI DSS compliance within 60 days.
   i. Merchants may be dependent on other University departments for assistance with compliance issues and will engage those departments for appropriate support as may be required. In some cases it may be appropriate that the supporting department defines and implements the corrective actions.
   ii. If the supporting department cannot provide corrective action within 60 days or less, the merchant will notify the PCI Steering Committee, which will escalate the issue to governance including the VPFA, the dean or director of the merchant and the dean or director of the supporting department.

b. Corrective actions will be monitored and approved by the PCI Steering Committee.
c. If corrective actions are not implemented within 60 days, or if the department challenges the non-compliance, the PCI Steering Committee will notify the Office of the VPFA.

d. The Office of the VPFA will apply sanctions as may be warranted by the situation.

11. **Employee Statement of Understanding.** Supervisors will ensure that employees who handle CHD as part of their employment or other activity at UNH attend initial and, at least, annual PCI DSS training and complete and sign the employee Statement of Understanding form provided by the merchant. The Statement of Understanding will be retained for at least 1 year or until the next training session is conducted.

12. **Annual Merchant Questionnaire.** Each merchant will complete and/or update an annual compliance self-assessment questionnaire (SAQ), taking necessary action to be able to attest compliance to the current PCI DSS.

13. **Best Practices.** The USNH Quality Security Assessor (QSA, as defined and required by PCI DSS) may provide guidance on best practices for USNH institutions to incorporate into merchant procedures to better understand and comply with the requirements of the standard. All UNH organizations that are subject to PCI DSS are expected to follow these best practices. Where conflict may exist between departmental guideline and practices and the QSA recommended practices, the UNH PCI SC will advise on reasonable resolution of the conflict.