University System of New Hampshire

PAYMENT CARD DATA SECURITY BEST PRACTICES GUIDE

Below is a summary of best practices recommended for all Payment card merchant locations and adopted by USNH.

1. **If you don't need it, Don't store it!**
   - Many offices retain cardholder data (CHD) 'just because.' Since we record each transaction number and date, you can always ask the acquiring bank for the CHD if you need it.
     This includes paper and electronic documentation. Once the transaction has been authorized, destroy the CHD on the form. This may require a redesign of the form to move the CHD to the bottom where it can be properly removed and cross-cut shredded.
2. **Destroy all CHD once a transaction is authorized**
   - All forms or paper with CHD should be shredded in a 'cross-cut' type shredder.
   - Third-party shredding services may be used, providing the bins that they provide are secure and cannot be removed from the area.
3. **Maintain a clean desk policy**
   - CHD should not be left out on desks or in open areas when not needed. Even if leaving the desk for a short period, staff should keep material in a folder and lock the folder in the desk when they leave temporarily. All CHD should be destroyed immediately after a transaction has been authorized.
4. **Do not store CHD electronically**
   - Do not copy or type CHD into spreadsheets or documents on general use workstations even for temporary use. Even if you don't save the document, an image or file of the data is stored on the hard drive.
5. **Never use any unencrypted electronic communication method such as email as a manner of transmitting Cardholder data.**
   - Should a customer e-mail their payment card information, reply to the sender deleting the payment card information from the reply, and inform them that 'for their protection and that of USNH, policies dictate that payment card information shall not be accepted via email. Please use one of our accepted methods of processing your information: (in-person, online, fax, form, etc.).'
6. **Do not allow unauthorized persons access to areas where payment card data is stored or processed.**
   - This includes other USNH staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This sometimes requires a change in service times.
7. **Document Desk Procedures**
   - To insure continuity when office personnel are out, have all individuals document daily procedures for their role in the handling of confidential data. Include such items as receipt and processing procedures, disposition and destruction of CHD, and storage/transfer of forms within the office.
8. **Online Payment Card Systems**
   - Many departments outsource card processing to third-party payment systems. In these situations, USNH should not routinely act as the customer and input customers' data in the third-party payment system for them.