BEST PRACTICES FOR OFFICES

We understand that complying with the PCI DSS may be difficult and confusing for some departments. We offer this set of best practices for you to implement into your office procedures to better understand and comply with the requirements of the standard.

1) **If you don't need it, don't store it!**
   - Many offices retain cardholder data (CHD) "just because." If you keep the transaction number and date, you can always ask the acquiring bank for the CHD if you need it.
   - This includes paper and forms. Once the transaction has been processed, 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) **Proper destruction**
   - 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) **Online Payment Card Systems**
   - Many departments employ the use of third-party payment systems to outsource card processing to an online process. Many times it is considered good customer service to take phone calls to process a credit card transaction.
     – It is not recommended to act as the customer and input their data for them.
     – When it is necessary to provide this service: CHD transactions must be conducted on a separate (isolated) payment terminal that is secured and monitored by Information Services.

4) **Maintain 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. At the end of the day, all CHD should be stored in a secure file cabinet or safe.

5) **Electronic storage of CHD**
   - 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.

6) **Never email Credit Card information**
   - Staff should never use email as a manner of transmitting Cardholder data
   - Should a customer email their credit card information:
     – Reply to the sender, deleting the credit card information from the reply and inform them that "for their protection the University of Richmond's policies dictate that credit 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)."

7) **Do not allow unauthorized persons unaccompanied access to areas where credit card data is stored or processed**
   - After normal work hours, all CHD must be locked in a secure cabinet or safe, accessible to only the authorized user. Neither maintenance nor janitorial personnel should have keys to the secure cabinet or safe.

8) **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; storage and transfer of forms within the office.