CAMPBELL UNIVERSITY

BEST PRACTICES

HANDLING PERSONALLY IDENTIFIABLE INFORMATION (PII)

North Carolina General Statute (NCGS) 75-60 Article 2A is specific to the NC Identity Theft Protection Act and defines personal information as a person's first name or first initial and last name in combination with identifying information as defined in NCGS14-113.20(b) which includes a social security number, employer taxpayer identification number, driver license number, state identification card, passport number, checking and savings account numbers, credit and debit card numbers, PIN codes, electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names, digital signatures, any other numbers or information that can be used to access a person's financial resources, biometric data, fingerprints, passwords, and the parent's legal surname prior to marriage. Personal information does not include publicly available directories containing information and individual has voluntarily consented to have publically disseminated or listed, including name address, and telephone number and does not include information made lawfully available to the general public from federal, state, or local government records.

We understand that complying with the PCI DSS, along with the protection of other Personally Identifiable Information (PII) 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 standards and federal regulations.

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.
    - Likewise, many offices retain other forms of personally identifiable information (PII) "just because". Review your processes. If you don't need it, don't keep it! Ask yourself, "Are multiple people in your area retaining the same data?" If so, limit the number of staff retaining the data to one person to be responsible for safeguarding the data.
2) **Proper destruction**
    - All forms or paper with CHD and PII data 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 CU departments employ the use a third party, such as CASHNet for online payment card processing. Many times it is considered good customer service to take phone calls, emails or some other form of communication 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: transactions should be conducted on a separate (isolated) payment terminal. **Contact the CU Computing Services Office for additional information regarding an isolated terminal.**

4) **Maintain clean desk policy**
    - CHD or other forms of PII data 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 and PII data should be stored in a secure file cabinet or safe in a locked office with limited access.
    - Forms used to collect CHD or PII data should be marked 'Confidential'.
    - Forms used to collect CHD or PII data should be printed on colored paper to assist with identifying sensitive information that must be safeguarded.

5) **Electronic storage of CHD and other PII data**
    - **Do not** copy or type CHD or PII data 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 CHD or other PII data**
    - Staff should never use email as a manner of transmitting CHD or PII 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 and the university'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, or by fax)." [Please note: Fax machines must be in a secured location. Employees should utilize passcodes to access faxes to ensure control of sensitive information.]

7) **Do not allow unauthorized persons unaccompanied access to areas where credit card data is stored or processed**
    - This includes other Campbell University staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This sometimes requires a change in service times.

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 and PII data. Storage and transfer of forms within the office.

9) Secure your computer –

- Campbell University requires that all users change network passwords every 90 days and follow these password creation rules:
    - Between 8 and 15 characters long
    - Must contain at least 3 of the following character types:
        - Uppercase
        - Lowercase
        - Numbers
        - Special Characters: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
- When leaving your office for any length of time, no matter how short, always lock your computer desktop by pressing the Ctrl, Alt, and Delete keys simultaneously and select "Lock this computer" from the menu and press Enter. You will be required to enter your password to unlock the computer.
- Never share your user name and password with colleagues or students. It is every user's responsibility to protect data.