

## **Policy on Data Handling**

As more and more data become stored electronically issues begin to arise as to the amount of personal and confidential content and its security. The purpose of this policy is to define the guidelines and handling of such data within Business Affairs.

### **Definitions of Restricted Data and Personally Identifiable Information (PII)**

Restricted Data are defined as data subject to restriction by Federal and State laws (i.e. FERPA, HIPAA). Some examples of restricted data include, but are not limited to, bank account information, student class schedules, grades, personnel records, etc. A more complete definition can be found at:

[http://its.uncg.edu/Technology\\_Procedures/Data\\_Classification/](http://its.uncg.edu/Technology_Procedures/Data_Classification/)

“Personally Identifiable Information (PII)” is defined by the North Carolina Identity Theft Protection Act to mean a person’s first name or first initial and last name in combination with any of the following items:

1. Social security or employer taxpayer identification number.
2. Driver’s license, State identification card, or passport numbers.
3. Checking account numbers.
4. Savings account numbers.
5. Credit card numbers.
6. Debit card numbers.
7. Personal Identification Number (PIN code).
8. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
9. Digital signatures.
10. Any other numbers or information that can be used to access a person's financial resources.
11. Biometric data.
12. Fingerprints.
13. Passwords.
14. Parent's legal surname prior to marriage.

PII/Restricted Data does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, email address, and telephone number, and does not include information made lawfully available to the general public from federal, State, or local government records.

## **Handling of Data**

### *Physical Records*

Physical records containing PII or Restricted Data must be stored in an appropriate type of locked space that has restricted access to just those personnel who need this information to perform their job functions. This may include but is not limited to, locked file space within the office. There is also locked space in the warehouse that is available for long term storage of these documents. These documents must be retained and disposed of as per the Business Affairs Policy on Data Retention.

Physical documents that are imaged, or data transferred from such documents makes this data electronic in nature, and the below “Electronic Information” requirements would govern that data. If at all possible, destroy the physical documents after the transfer of information to electronic form. Please keep in mind that documented evidence that the electronic records were created, reproduced, and otherwise managed in such a manner as to ensure the reliability, accuracy, and security of both the records and the process or system used to produce the records is required. It is understood that some physical documents may have required retention times based on state requirements. Please see the policy on Data Retention for more information on the retention, storage, and disposition of these documents.

### *Electronic Information*

Access to PII/Restricted Data shall be limited to those personnel that need this information to perform their job functions. The authorization for the access of this data shall be done with Employee, Department Head, and data steward (or their agent) signatures/approvals.

As a rule, no one should save any PII/Restricted Data on a computer hard drive. If it is necessary to save PII/Restricted Data, any saving and storage should be done on a network volume only accessible by the user saving the information or other employees with a business justification and authorization for accessing the saved PII/Restricted Data. If at all possible, PII/Restricted Data accessed electronically should NOT be stored on local computers. If it is necessary to store PII/Restricted Data on a local computer, it must be deleted as soon as possible, using a data overwrite tool such as Eraser. PII/Restricted Data should *never* be saved on a computer without such a tool. In addition, no PII/Restricted Data should ever be saved unencrypted on ANY portable data device, such as a portable hard drive, usb/thumb drive, writable CD/DVD, etc. Also, no encrypted PII/Restricted Data should ever be saved on a portable computing device (laptop, PDA, Blackberry, etc.) except in cases of extreme emergency, i.e., the implementation of Business Affairs Business Continuity Plan.

Under no circumstances should PII/Restricted Data be sent via email in the body of an email or as an unencrypted email attachment. Password protected Word and Excel documents are easily accessed and do NOT qualify as encrypted attachments. Email is an inherently unsecure mode of communication, and can be fairly easily accessed by outside intruders. Likewise, such information should not be transmitted over the internet in any unsecure form. SFTP and HTTPS are the only currently available methods for transmitting PII/Restricted Data securely over the internet. Other vendors may provide their own secure transport mechanism that may be used. Likewise, no PII/Restricted Data should ever be posted to any website, public or private.

As a matter of security, no software should be installed on any University machine apart from the standard university drive image or other University approved software (i.e. WebFocus), unless the software has been approved by BOTH the appropriate Assoc. Vice Chancellor AND the Director of Business Affairs Technology.