SECURING PERSONALLY IDENTIFIABLE INFORMATION

SCOPE

Northwood University, its employees and vendors have an ethical and sometimes legal responsibility to protect the personally identifiable information of its constituents. The purpose of this policy is to define Personally Identifiable Information (PII) and standards for its use, storage and disposal.

POLICY

Personally Identifiable Information (PII):
Defined as an individual's name, address, or telephone number combined with any of the following:

- Social security number or taxpayer ID number
- Driver's license number
- Account Number
- Credit or debit card number
- Access codes, security codes, passwords or any combination of an individual’s information that would permit access to an individual’s PII
- Financial information protected under GLBA
- Medical or health information protected under HIPAA
- Student related data protected under FERPA

PII will not be disclosed except as provided by University policy and procedure or legal disclosure requirements. PII will be protected and secured in accordance with the following standards.

How to Protect Personally Identifiable Information:

Electronic Storage and Disposal

- Do not transmit PII via email or the Internet unless the connection is secure or the information encrypted. Any encrypted communications must be setup and approved by Information Technology.
- Do not store PII on a PDA, USB drive, CD, flash memory card, floppy drive or other portable storage media unless the PII has been encrypted using a system setup and approved by Information Technology.
- Do not store PII on your laptop or desktop computer’s hard drive unless the PII has been encrypted using a system setup and approved by Information Technology. Exceptions may be granted in cases where employees do not have access to server storage when working in offsite locations.
- Do not store PII in public files accessible via the Internet or Intranet. Examples would be publicly available web pages, unsecured drive shares and course management classes.
- Do not download PII from Northwood University databases unless there is a legal or business requirement to do so. If download files are required, they should be stored on a University server (samba, s drive or group server share)
- Destroy media (such as disks, tapes, hard drives) that contain PII in a manner that protects the confidentiality of the information.

Physical Storage and Disposal

- Do not publicly display PII or leave PII unattended. This includes but is not limited to leaving PII on your desk or on the desk of a co-worker.
- Do not take PII home.
- Lock offices, desks, and files that contain PII when unattended.
- Shred PII when it is no longer needed. Do not discard PII in the trash without properly shredding the documents beforehand.

**Security**

- Lock or log off your computer when unattended.
- Eliminate the use of PII on forms whenever possible.
- Do not share passwords and do not document passwords.
- Never provide your password to anyone, including IT employees or someone claiming to be an IT employee. Authorized IT staff members have full access privileges and do not need to know individual user’s passwords.
- The Gramm-Leach-Bliley act, FERPA and HIPAA laws should be followed when dealing with confidential or private information.

**Legal Disclosure Requirements**

- Do not share PII documents or information with anyone unless required by government regulations, specific NU job responsibilities or business requirements. Be prepared to say “no” when asked to provide that type of information.
- Do not communicate confidential student information designated by the FERPA flag.
- Notify Northwood University Information Security Manager, Director of Information Technology or Vice President of Finance immediately if you suspect PII may have been compromised.

**REFERENCES**

Current Information Security Manager: Jim Beechey beechey@northwood.edu 989-837-4169
Current Director of Information Technology: Bob Wisler bwisler@northwood.edu 989-837-4435
Current Vice President of Finance: Don Hunkins hunkins@northwood.edu 989-837-4211

Texas Christian University “Securing Sensitive Personal Information”