Cheyney University Policy FA 2013-4033

Policy on Sensitive and Confidential Information

Approved: Finance and Administration Council / President's Cabinet

History: Issued—March 12, 2013

Related Policies: Policy FA-2010-4027 Policy on Record Retention

Additional References: n/a

A. PURPOSE

The purpose of this policy is to clarify the collection, processing, storage or dissemination of sensitive personal information.

B. SCOPE

All University records.

C. DEFINITION(S)

SI: Sensitive Information. Any document or record that contains personal information that can be used as identification of an individual.

HIPPA:Health Insurance Portability and Accountability Act.

FERPA:Family Educational Rights and Privacy Act.

D. POLICY AND PROCEDURE(S)

Cheyney University requires all employees to protect sensitive Information (SI) to prevent unauthorized use.

Sensitive Personal Information includes:

- Social security numbers or taxpayer ID numbers
- Credit card information
- Driver's license
- Date of birth
- Passwords and passcodes (electronic devices, computer, mobile, software files- Word, Excel, SAP, PowerCampus, etc- building and room alarm codes, voicemail codes, door access codes)
- Employee and student ID numbers
- Employee and student home phone, cell phone and home addresses.
- Any medical information protected under HIPPA or student data protected under FERPA

Employees will secure Sensitive Personal Information (SPI) as follows:

Physical Storage:

- Do not leave SPI on public display or unattended at your desk.
- Shred SPI when no longer needed.
- Lock files containing SI.
- Do not take home files containing SI.

Electronic Storage:

- Use password protection to store files containing SPI.
- Do not download SPI onto other storage media unless authorized by a supervisor and then secure the media under lock and key, discard media in a manner that protects the information.
- Do not transmit SPI to third parties via Internet, e-mail or wireless technology.
- Receive authorization from a supervisor to transmit any SI electronically.
- If your computer contains SI, lock machine when unattended using Control, Alt, and Delete which requires a password to unlock the machine.

Sharing of Information:

- Do not share SI documents with anyone unless authorized by your supervisor.

Retention of Information:

- Follow Cheyney University Policy AF-2010-4027 policy on record retention.

Notification:

- Any detection of breach shall be reported immediately and written notification will be sent first-class mail within seven (7) days to all intended parties.