SOWELA
TECHNICAL COMMUNITY COLLEGE
www.sowela.edu

TITLE: Data Security on Portable Storage Devices

EFFECTIVE DATE: April 7, 2009
LAST REVISION: November 10, 2017 **Policy No. 7.002.2**

Purpose:
The purpose of this policy is to establish a standard for securing SOWELA Technical Community College's data on movable devices and to comply with the State of Louisiana Office of Information Technology Policy IT-POL-014 to protect sensitive, proprietary and other data not subject to the Louisiana Public Records Act (LA.RS 44:1 et seq.) [Hereafter referred to as sensitive data] on agency approved notebook PC's and portable data storage devices that are removed from state premises.

Policy:
All sensitive data that is stored on agency approved portable storage devices (Notebook PC's, laptops, USB thumb drives, USB hard drives, CD's, DVD's, diskettes, PDA's, tablets, smart phones, etc.) that are removed from the SOWELA Technical Community College (SOWELA) premises must be encrypted in consistent with OIT STD 023 (Encryption Standard).

Scope:
All full-time, adjunct, and/or temporary employees of SOWELA must comply with this policy.

Definition:
Sensitive Data is defined by SOWELA as all data containing employees and/or students personal information. All financial aid information, all student record information, all human resources information, all information from finance that concerns student information, and any information that faculty may have in history files containing student social security records.

Responsibilities:

- Supervisors must document a business case to support employees or contractors taking sensitive data off SOWELA premises.
- Supervisors must make reasonable assurances that only SOWELA approved storage devices will be used if employees or contractors are allowed to take sensitive data off SOWELA's premises.
- Supervisors must make reasonable assurances employees subject to this policy are aware of the proper techniques regarding use of encryption on the devices referenced above.
- Supervisors must make reasonable assurances contractors utilize encryption consistent with OIT STD 023 when taking sensitive data off state premises.

Source of Policy: Information Resources &Technology Department
Responsible: Administrator: Chief Information Resources & Technology Officer
Related Policy: N/A
LCTCS Policy Reference: N/A
LCTCS Guideline Reference: N/A

Approved by: _____
Chancellor
Date: 2-5-18