Policy # 56002

DATA SANITIZATION POLICY

Effective Date: June 19, 2009 **Revised Date:** February 6, 2023
Responsible Office: Information Technology Center
Division: Finance

I. PURPOSE/OBJECTIVE

The purpose of this policy is to protect the university by removing sensitive data from Grambling State University desktops, laptops, digital devices, and removable media. For the purpose of this policy Grambling State University will follow the standards and guidelines of the Office of Information Technology (OIT) IT POL 1-04.

II. STATEMENT OF POLICIES

A. This policy applies to, but is not limited to, all devices that fit the following device classifications:

1. Portable and notebook computers running Windows, UNIX, Linux, or Mac OS operating systems.

2. Workstations running Windows, UNIX, Linux, or Mac OS operating systems.

3. Removable media defined as:

   Portable USB-based memory sticks (flash, thumb, jump, or key drives).

   Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.

   USB card readers that allow connectivity to a PC.

   Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.

   PDAs, cell phone handsets, and smartphones with internal flash or hard drive-based memory that supports a data storage function.

   Digital cameras with internal or external memory support.

   Removable memory-based media, such as rewritable DVDs, CDs, floppy disks, and tapes.

Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access.

Portable hard drives, DVD, or CD.

B. This policy applies to all computers, digital devices, removable media owned or leased by Grambling State University and capable of storing sensitive data or information related to the privacy of employees, clients, or suppliers.

1. All computers, digital devices, and cell phones transferred **internally** must be sanitized. Upon approval of the Unit/Department Head computers may remain the same, the Data Sanitization form must be completed.

2. All computers transferred **externally** will go to property and receiving. ITC will sanitize computers according to the methods defined in this policy. This scenario includes computers transferred to another department, computers returned to a vendor for servicing or maintenance and computers released to an external agency for disposal.