# Policy # 56010

## REMOVABLE MEDIA USAGE/DATA TRANSPORT POLICY

**Effective Date:** March 2012 **Review Date:** January 1, 2022
**Responsible Office: Information Technology Center**
**Division: Operations**

### I. PURPOSE/OBJECTIVE

The purpose of this policy is to establish the principles and working practices that are to be adopted by all legitimate end users associated with the risk of connecting portable removable media to any infrastructure within Grambling State University's internal network(s) or related technology resources and transporting sensitive data. This removable media and data transport policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications and follow the standards and guidelines of the Office of Information Technology (OIT) IT POL1-22 and IT STD 1-13, ITC Data Classification Policy #56003, ITC Password Policy #56004:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, 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 support 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.
- Notebooks/Laptops

## II. STATEMENT OF POLICIES

This policy applies to all Grambling State University's employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either university-owned removable media and/or USB-based technology to store, back up, relocate or access any organization or university-specific data, or transport sensitive data.

This policy addresses a range of threats/risks of using or transporting sensitive university data:

| Threat | Description |
|---|---|
| Loss | Devices used to transfer or transport work files could be lost or stolen. |
| Theft | Sensitive university data is deliberately stolen and sold by an employee. |
| Copyright | Software copied onto portable memory device or laptop could violate licensing. |
| Spyware | Spyware or tracking code enters the network via memory media. |
| Malware | Viruses, Trojans, Worms, and other threats could be introduced via external media. |
| Compliance | Loss or theft of financial and/or personal and confidential data could expose the university to the risk of non-compliance with various identity theft and privacy laws. |

Each user is responsible for the appropriate use, security of data, and not allowing removable media devices and the data stored on these devices to be compromised in any way while under their control.

All users assume the responsibility to insure all removable media is free of virus and malware.

It is the responsibility of the hosting department to insure that non-agency personnel do not use removable media in an unauthorized fashion.

**Policy Non-Compliance**

Non-compliance with this policy could have a significant effect on the efficient operation of the university and may result in financial loss and an inability to provide necessary services to our faculty, staff, and students.

The ITC will be responsible for reporting any breach of this policy to the respective Vice President.

## III. REVISION/REVISED HISTORY

March 2012-Effective Date