1.6 - Bring Your Own Device (BYOD) Standard

Introduction

The purpose of this standard is to establish accepted practices, responsibilities, and procedures for the use of personally owned devices that West Virginia University at Parkersburg authorizes to connect to college computer and network systems. This standard defines the user requirement, and provides guidance for the securing mobile devices, such as smartphones and tablets.

Standard

The following controls must be applied to mobile devices that connect directly to the West Virginia University at Parkersburg network and/or access WVUP-owned data:

- Passcode or password security must be active on the device.
- Any credentials used to access various college data sources (WVUP Network ID, Banner password, etc.) must be changed immediately upon the event of a lost or stolen device that has been configured to access college services or data.
- Safeguards should be taken to remotely erase data stored on the device in the event of theft or loss if available.
- Devices that are jailbroken, "rooted," or have been subjected to other methods of changing built-in protections are not permitted to access WVUP resources.
- Users must take appropriate precautions to prevent others from obtaining access to their mobile devices. Users will be responsible for all transactions made with their credentials, and must not share individually assigned passwords or other credentials.

Violations

Violation or non-compliance of this standard will be addressed in accordance with established college disciplinary policies and procedures, as issued and enforced by the appropriate authorities. Failure to comply with this or other related standards may result in disciplinary action up to and including termination of one's employment or duties.