1.10 - Multi-Factor Authentication Requirement Policy

Purpose

West Virginia University at Parkersburg interacts with various forms of sensitive data. In order to better protect this information, users with access to this data are required to use additional security measures.

Definitions

- Personally Identifiable Information (PII) - information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples include Social Security Numbers and Driver's License ID numbers.
- Data store - repository for persistently storing and managing collections of data which include not just repositories like databases, but also simpler store types such as simple files, emails etc.
- Multi-factor Authentication - electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).
- Information system - a computer system or set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself.

Policy

- All user accounts (staff, faculty, or student employee) with access to data stores housing Personally Identifiable Information are required to be set up with multi-factor authentication.
- Information Technology determines whether or not this is required, depending on what data stores and information systems the user has access to.
- All mobile devices used as authenticators must have screen locking and passcode/biometric security set up
- In the event of a lost or stolen authenticator device, IT must be notified immediately so that the device can be de-registered.
- Information Technology reserves the right to prohibit authenticator devices that do not meet security requirements.