1.2 - WVUP Account Management Policies

Purpose

This policy establishes how user accounts are created, modified, and deleted.

Scope

This policy applies to all faculty, staff, and students.

Policy

User Accounts

- West Virginia University at Parkersburg IT staff are responsible for creating, modifying, and deleting all accounts.
- All faculty and staff accounts must include an electronically submitted form by Human Resources.
- Student accounts are programmatically generated from Banner. Accounts are created multiple times throughout the day.
- WVUP IT will issue a unique account to each authorized individual that will be deactivated when necessary.
- When creating accounts, the principle of "least privilege access" will be used. Users will be granted access to network resources and data required to perform job duties.
- Unless otherwise authorized by WVUP IT, account sharing is prohibited. Users must use their individual IDs to access network resources and data.
- Each department and division will have an identified employee responsible for requesting access modifications.
- WVUP IT will periodically audit existing user accounts to ensure that access and account privileges are still appropriate based on job function, "need to know", and employment status.

Temporary Accounts

- Accounts for contractors and temporary employees will be created as needed following the principle of least privilege.
- Temporary accounts will be set with an expiration date of one year unless otherwise requested.
- All temporary accounts must be authorized by the appropriate supervisor or entity responsible for the temporary employee.

Shared Accounts

- While shared accounts are generally prohibited, some systems require a single administrative account. In these situations, responsible users must ensure that these passwords are only shared with the appropriate personnel and properly secured.
- If at any time a user with access to a shared account leaves, the password for that account must be changed immediately.

Application and System Standards

- Shared accounts are not permitted unless specifically required by the application or business purpose.
- Authentication should take place external to the application. External authentication services, preferably Active Directory, should be used.
- Passwords cannot and will not be stored in plain text.
- Role-based access controls should be used whenever feasible, to accommodate changes in staff or assigned duties.
- Where technically or administratively feasible, systems should allow for account lock-outs after a set number of failed attempts and log the failed attempts.