1.11 - Password Policy

Information security is a vital component of the Office of Information Technology at West Virginia University at Parkersburg. As such, it is very important that all users follow established password policies and best practices.

Overview

These guidelines will reduce the risk of a data breach at West Virginia University at Parkersburg.

Password Complexity

- All users' passwords must be at least ten characters

Password History

- Passwords may not be re-used. A history of the last ten passwords will be kept and the password management system will prevent the re-use of passwords recently used.

Password Security

- All users are expected to not share account credentials with anyone.
- All users are expected to secure account credentials.

Password Expirations

- For employees using Multi-Factor Authentication, password changes are required once every 365 days.
- Password changes are required for all other users once every 180 days.
- Users will be notified via email a week before their password is set to expire. Included in the email will be a link to the password management system that will allow users to change their password.
- Users will continue to receive reminder emails, either until the password has been changed or the deadline is reached.
- In the event that the password is not changed, and the deadline has been reached, the account will be disabled until the user changes the password.

Exceptions

Exceptions to this policy may be made at the discretion of the Chief Information Officer. A formal email must be sent to the Chief Information Officer with the affected user's full name and justification for the exception.