D. Passwords/passphrases should not be written down. The University will provide a secure password manager for University community members use.

E. Password Requirements

1. Passwords/passphrases must be a minimum of fifteen (15) characters.
2. Passwords/passphrases expiration shall be set to 365 days for non-MFA enabled accounts, for MFA-enabled account, a password/passphrase reset is only required upon potential or confirmed password compromise.
3. Passwords/passphrases shall lock after five (5) failed attempts. Automatic reset shall be set at five (5) minutes.
4. Passwords/passphrase history shall be set to last eight (8) passwords and the same password/passphrase cannot be re-used within the last two (2) years.
5. Users shall be notified at least two (2) weeks before their password/passphrase is about to expire.
6. When a password/passphrase reset is requested, the reset request will not be processed until