OFFICE OF INFORMATION TECHNOLOGY (OIT)
Policies and Procedures Manual

1.2. Password / Passphrase Security Policy

1.2.. Purpose

1.2.1. To provide a mechanism to maximize the security of information stored on University technology through the appropriate use of passwords / passphrases. Both words (passwords and passphrases) will be used interchangeably in this policy, but are two separate terms.

1.2.2. Passwords are assigned to each individual as a method to control and monitor their unique access to systems and information, and should never be shared with others.

1.3. Policy

1.3.1. Passwords will be changed frequently, currently every six months.

1.3.2. Users must change their password immediately upon the suspicion or knowing it has been compromised.

1.3.3. Users must immediately report any suspicious or suspect activity involving their accounts or other activity to the Help Desk.

1.3.4. Users are not to give others access to systems or information by providing them with their account and password at any time.

1.3.5. Users will be held individually responsible for the actions of others if they have knowingly shared their password and access with them.

1.3.6. Procedure

1.3.7. Where possible, the Office of Information Technology (OIT) will implement automatic password expiration processes to ensure passwords are changed on a regular and timely basis.

1.3.8. Where possible, OIT will implement password complexity rules on each system. However, if not possible, passwords should adhere to the following:

1.3.8.1. Make each password unique – do not use the same password for multiple accounts or systems;

1.3.8.2. Make the password at least 8 characters long (the longer the better);

1.3.8.3. Use at least one number (0-9);

1.3.8.4. Use at least one upper (A-Z) and one lower case (a-z) letter;

1.3.8.5. Use at least one symbol (!,#,$,^) that the system supports

1.3.8.6. Do not use standard words that would be listed in a dictionary (even non-American English words);

1.3.8.7. Do not use simple transformations of words such as Tiny8 or 7Eleven or alphabetic or numeric sequences such as abcdef or 12345

1.3.8.8. Do not use any personally identifiable information or passwords or phrases that may be easy to guess;

1.3.8.9. Use long passphrases instead of small overly complex passwords. For example ‘Another1longpass!’

1.4. Enforcement

1.4.1. Violations of any part of this policy may result in disciplinary action as prescribed by University policies and procedures.

1.5. Approval and adoption

1.5.1. Approved by the Chief Information Officer and Executive Vice President and adopted effective 10/15/2002.

1.5.2. Updated to accurately reflect current password requirements and standards used in Active Directory. Reviewed and approved by the Chief Information Officer and Vice President for Facilities & Technology Services and adopted effective 11/1/2017.

1.5.3. Updated of terminology and technologies and move approvals to the end of document. Reviewed by Senior Directors of Infrastructure and Enterprise Applications, and CIO and adopted effective 7/1/2020.

1.5.4 Reviewed by AVPs of Infrastructure and Systems, Enterprise Applications, and CIO with no changes made as of 7/1/2023.