1.2. Password / Passphrase Security Policy

1.2.1. Approval and adoption

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

1.2.1.2. 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.

1.2.2. Purpose

1.2.2.1. 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.

1.2.2.2. 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.

1.2.3. Policy

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

1.2.3.2. Users will change their password immediately upon suspecting or knowing it has been compromised.

1.2.3.3. Users are not to give others access to systems or information by providing them with their account and password.

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

1.2.4. Procedure

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

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

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

1.2.4.2.2. Make the password at least eight characters long (the more the better);

1.2.4.2.3. Use at least one number;

1.2.4.2.4. Use at-least one upper case and one lower case;

1.2.4.2.5. Do not use standard words that would be listed in a dictionary (even foreign words) – there are programs designed to break passwords by using all words in a dictionary;

1.2.4.2.6. Do not use simple transformations of words, such as Tiny8 or 7Eleven; and

1.2.4.2.7. Do not use alphabetic sequences such as abcdef.

1.2.4.2.8. Use long passphrases instead of small overly complex passwords. For example ‘Horsejumping13’ is a more secure password than ‘H0r$eJ13’ and is also easier to remember.

1.2.5. Enforcement

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