Security Standard: Password/Passphrase

Scope

This standard applies to RIT account passwords/passphrases.

Requirements

Passwords for the accounts of users and administrators on RIT computing and networked resources are required to *meet the requirements below to the maximum allowable* by the device or application:

1. **Password Complexity**
   - 1.1. Passwords should be at least 8-characters. A longer passphrase is preferred. (A passphrase is a sequence of words or other text.)
   - 1.2. Passwords should contain both upper and lower case letters, at least one number, and one special character.

2. **Password Protection**
   - 2.1. The user or administrator is the sole custodian of the password and should protect the password at all times.
   - 2.2. Passwords should be physically secured if written down and should be encrypted if stored or transmitted digitally.
   - 2.3. Passwords should not be shared, unless used for a documented and approved shared account.
   - 2.4. Passwords used for RIT accounts shall not be used with non-RIT accounts.

3. **Password Changes**
   - 3.1. Passwords should be changed *at least* annually
   - 3.2. Passwords should not be reused for the next 6 password changes.
   - 3.3. Passwords should be changed immediately when:
     - The password is a default or temporary password created by someone other than the user. This includes generic, vendor-supplied, and help/service desk default passwords.
     - The password, or a system, service or application storing, processing or transmitting the password, is suspected to have been shared or compromised.

Effective Date: January 23, 2015

Standard History:
June 21, 2004