Statement of Policy

Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective

This policy provides direction for authentication to WashU systems and network.

Policy

In order to connect to WashU systems or network all account holders must comply with the following:

- Credentials (i.e. passwords, pins, passphrase) must be random and required to change on the first login.
    - Passwords are not to be shared.
    - Default passwords will not be given to all workforce members.
    - Multifactor authentication will be used when available.
- WashU IT Support groups will only reset password when the identity has been verified.
- WashU IT Support groups will not ask for workforce member's password via email.
- WashU account holders
    - will refrain from writing passwords down.
    - will not send their WashU issued accounts and / or passwords in an email without encryption.
    - will not use the same passwords for WashU that are used for personal accounts.
    - will not circumvent authentication with auto logon, application remembering, embedded scripts or had coded authentication credentials in client software except where approved by the Information Security Office.
    - will contact the WashU IT Support group to reset your passwords if you suspect it has been compromised.
- WashU passwords will not be stored or remembered by applications, especially when not using your normal workstation (i.e. kiosks, common workstations, friends or families computers)
- Password protected screen savers or logging off the device is required when systems are unattended.

Password Requirements

- Minimum 8 character passwords
- Any lower case letters (a-z)
- Any upper case letters (A-Z)
- Any numbers (0-9)
- Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (!@#$%^&*()_+=={}[]:;"'|\/?<>,.~`)

- Passwords must not include easily guessed information (personal information, names, pets, birth dates, etc.) or words found in a Dictionary

Password Expiration

Individual user passwords must be changed (i.e. expire) at least every 120 days
Individual user passwords with MultiFactor enabled must be changed (i.e. expire) at least annually

EXcEPTIONS

If a system does not support the minimum structure and complexity as listed above, an exception form must be completed and a risk assessment will be performed by the WashU Information Security Office.
Where software permits:

- Require that files containing authentication are one-way encrypted.
- Require authentication to be entered in non-display fields.

Title: Password Policy
Version: 2.0
Creation Date: November 20, 2007
Applicability: Confidential and Protected
Reference Number: 02.07
Status: Final
Revision Date: April 6, 2016
Policy Owner: Information Security Office