Password Policy

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
The policy and associated guidance provide direction for authentication to WashU systems and network.

Applicability
This policy is applicable for authentication to all WashU network segments.

Audience
The audience for this policy is all WashU faculty, staff and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

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

- Credentials (i.e. passwords, pins, passphrase) will be random and required to change on the first login.
  - Passwords will not be shared.
  - Default passwords will not be given to all workforce members.
  - Multifactor authentication will be used when outside the WashU network.
  - Multifactor authentication may be required for all connections to the WashU network based upon job roles and requirements.
- IT Support groups will only reset a password when the identity has been verified.
• 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 their 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.

WUSTL Key is the preferred method of authentication for WashU systems and network.

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 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 (ISO).
Where software permits:

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

**Policy Compliance**
The ISO will measure the compliance to this policy through various methods, including, but not limited to - reports, internal\external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the ISO in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources or the Office of Student Conduct.

**Related Policies**
None

**Reference**
None

**Policy Review**
This policy will be reviewed at a minimum every three years.

**Title:** Password Policy  
**Version Number:** 3.0  
**Reference Number:** IA-01.01  
**Creation Date:** November 20, 2007  
**Approved By:** Security and Privacy Governance Committee  
**Approval Date:** April 6, 2016  
**Status:** Final  
**Scheduled Review Date:** March 1, 2022  
**Revision Date:** February 26, 2019  
**Revision Approval Date:** March 15, 2019  
**Policy Owner:** Information Security Office