Password Management Policy
Policy Purpose

Strong and secure passwords are key to protecting the university’s data. The purpose of this policy is to help guide system users in securing credentials used to access Wright State computer systems.

Policy Description

The following are general password policies applicable for network, system resources and Internet access use:

Users must abide by policies stated in the WSU Computing and Telecommunications Account Policy Statement.

Campus passwords and user logon IDs should be unique to each authorized user.

Campus passwords will follow the standard set forth on the WINGS portal.

- The password length must be 8 to 24
- The password must contain a letter.
- The password must contain at least one of these special characters:0123456789^(-)_!$
- Do NOT use names or common words in the dictionary.
- Do NOT use the last four digits of your SSN.
- Do NOT use your CAMPUS Account username, your first name, or your last name.
- Do NOT use 3 or more repeated (i.e., aaa or 111) or consecutive (i.e., abc or 123) characters.
- Must NOT be a previously used password.

Campus passwords will be kept private i.e., not shared, coded into programs, or written down.

Campus passwords will be changed every 180 days for employees, with the exception of individuals enrolled in two-factor authentication. Individuals utilizing two-factor authentication will not be required to change their password unless compromise of the password has occurred. Systems will enforce password change with an automatic expiration and prevent repeated or reused passwords. Student passwords will be changed every five years.

Campus passwords associated with the PCI-DSS systems change every 90 days. Systems will enforce password change with an automatic expiration and prevent repeated or reused passwords for a minimum of 8 previous passwords.

Campus User accounts will be locked after 9 failed logon attempts. User accounts associated with PCI-DSS systems will be locked after 5 failed logins requiring an admin reset. All failed login attempts will be recorded.

Successful logons should display the date and time of the last logon and logoff.

Logon IDs and passwords are suspended if a client is not authorized during current term unless authorized by Computing and Telecommunications Account Policy Statement.
Campus passwords will be changed after first use.