WRIGHT STATE UNIVERSITY

PASSWORD MANAGEMENT
CATS - INFORMATION TECHNOLOGY

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.1	7-9-08	Mike Persina	Initial Publication
1.2	2-16-09	Mike Persina	Annual Review/Modification
1.3	6-2-10	Mike Natale	Annual Review/Modification
1.3	10-4-11	Mike Persina	Annual Review – no changes
1.4	4-3-12	Mike Natale	Annual Review – Added PCI-DSS password reference
1.5	9-24-12	Mike Persina	Annual Review – Added 'First Use' verbiage.
1.6	3-6-13	Mike Natale	Added PCI-DSS reference lockout and repeat usage.
1.6	4-9-2014	Ken Nelson	Annual Review
1.6	05-25-2015	Michael Natale	Annual Review
1.6	08-01-2016	Michael Natale	Annual Review
1.7	10-01-2017	Michael Natale	Faculty and Staff enrolled in 2FA will not be required to change their password. Max character length changed.
1.7	02-01-19	Michael Natale	Annual Review
1.8	2-6-2020	John Remley	Annual Review and minor modifications.
1.8	9-21-2021	John Remley	Annual Review
1.8	4-21-2022	Michael Natale	Annual Review
1.8	5-1-2023	Michael Natale	Annual Review
1.8	2-23-2024	Mike Natale	Annual Review

WRIGHT STATE UNIVERSITY	**Wright State University** Information Security	WRIGHT STATE UNIVERSITY

Controls	
Policy Title:	Password Management Policy
Category:	Information Technology
Audience:	WSU Faculty, Staff, and Students
Reason for Revision:	*N/A*
Created / Modified Date:	2-16-09
Location:	http://www.wright.edu/security/policy/

Responsible Parties	
Author	Mike Persina
Technical Reviewer/Mgr	Matt Hemker

TABLE OF CONTENTS

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: wings.wright.edu

- 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.