



REGULATION TITLE:

Passwords

APPLIES TO:

All users of KSU information technology resources

ADMINISTRATIVE AUTHORITY:

Chief Information Officer (CIO)

Department of Information Technology (IT)

APPROVED BY:

Kentucky State University Board of Regents

EFFECTIVE DATE:

August 8, 2025

NEXT REVIEW DATE:

August 8, 2028

REGULATION STATEMENT:

This regulation establishes the minimum requirements for the creation, protection, and management of passwords used to access Kentucky State University's (KSU) Information Technology (IT) resources. The intent of this regulation is to safeguard university systems and data from unauthorized access and misuse by enforcing strong password standards.

DEFINITIONS:

Password

A secret word or string of characters used for authenticating the identity of a user to gain access to a protected IT resource.

Multi-Factor Authentication (MFA)

A security process that requires more than one method of authentication from independent categories of

credentials to verify a user's identity.

PROCESS:

Password Creation Requirements

A strong password is long and contains a mix of letters, numbers, and special characters. All passwords used to access KSU IT resources must meet the following requirements:

- Be a minimum of 12 characters in length.
- Contain at least one character from any of the following categories:
- Contain an uppercase alphabet character (A-Z)
- Contain a special character (*, %, !, etc.)
- Contain a numeric character (0-9)
- Must not contain any part of the user's account name.
- Cannot match any of the user's last three (3) passwords.

Password Protection and Handling

Users are responsible for maintaining the confidentiality of their passwords. The following protection rules apply:

- Passwords shall be treated as confidential information and must not be shared with anyone.
- Passwords must be promptly changed if they are suspected of being compromised.
- Passwords must not be written down or stored in an insecure manner (e.g., taped to a monitor). If a password must be stored, an encrypted password manager must be used.
- Passwords should not be emailed with usernames.
- Users must not save passwords in web browsers or use the "remember password" feature in applications.
- Users should not use their KSU password for any non-KSU accounts.
- The KSU IT department will never ask for a user's password.

System Security Controls

- After three (3) failed password attempts, a user's account will be locked out.
- Password-protected screen savers are mandatory on all university-owned computers and must be set to a maximum timeout of fifteen (15) minutes.

Frequency of Password Changes

KSU network passwords will expire every 180 days. Users will receive a notification prompting them to change their password beginning fourteen (14) days prior to expiration.

Password Reset Procedure

- **Self-Service:** Users may reset their own password at any time by using the password self-service system at www.kysu.edu/resettool. Users must be enrolled in the system prior to its use.
- **IT Help Desk:** Users may also have their password reset by contacting the IT Help Desk during business hours (8:00 AM – 4:30 PM). The user will be required to verify their identity with information such as their 8-digit KSU ID, the last four digits of their Social Security number, or by presenting a photo ID.
- **Compromised Accounts:** If a password has been compromised, IT will reset the password and enroll the account in multi-factor authentication.

Enforcement

Any individual who violates this regulation may be subject to disciplinary action, including but not limited to termination, loss of data-access privileges, administrative sanctions, and personal civil and criminal liability.

REFERENCES AND RELATED MATERIALS:

- KSU Information Security Policy
- NIST Special Publication 800-63B

CONTACTS:

Subject	Office	Telephone	E-mail
General Questions	Office of the CIO	(502) 597-7000	Wendy.Dixie@kysu.edu

HISTORY:

Revision Type	Date of Issuance/Revision	Drafter(s)/Editor(s)
Issued (New Policy)	May 2020	Unknown
Substantive Revisions	December 18, 2023	Wendy Dixie and Zach Atwell
Minor Revisions (New Template)	June 2025	Wendy Dixie and Zach Atwell