KENTUCKY STATE UNIVERSITY

KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

POLICY TITLE:
IT Password Policy

VOLUME, SECTION & NUMBER:
4.2.11

ENTITIES AFFECTED:
Students
Faculty
Staff
Individuals Using KSU Technology Services or Resources

ADMINISTRATIVE AUTHORITY:
Information Technology
Department of Finance & Business Affairs

APPROVED BY:
Kentucky State University Board of Regents

EFFECTIVE DATE:
December 18, 2023

REVISED FROM:
May 2020 Version of Policy

POLICY STATEMENT:

The purpose of this policy is to establish minimum requirements for the creation of passwords, the protection of passwords, the resetting of passwords, and the frequency of changing passwords. The intent of this policy is to ensure the appropriate protection and safeguarding of Kentucky State University's Information Technology (IT) resources and systems from unauthorized access and misuse.

PROCEDURES:

Passwords are one essential piece of computer security. Passwords (single authentication) or two-factor authentications (password and token) must be used to authenticate access into any system or application that contains confidential or restricted information.

Creation of Passwords

One of the most important actions you can take to protect you and your information from hackers is to have a strong password that is difficult to guess. A strong password is a password that is long and contains a good mix of letters, numbers, special characters, and both upper- and lowercase letters.

Password Requirements:

1. Passwords are case sensitive.
2. Password requirements are as follows:

    - Passwords must be at least 12 characters in length.
    - Passwords must contain at least one of the following:

        - Uppercase alphabet character (eg. A, C, Q, etc.);
        - Special character (eg. *, %, !, etc.); or
        - Numeric character (eg. 1,2,4, etc.)

    - Must not contain any part of your account name
    - Cannot match any of your last 3 passwords

Protection of Passwords

1. Passwords shall be treated as confidential information and shall not be shared with anyone.
2. Passwords will only be administered to the user of the account after proper verification.
3. All passwords must be promptly changed if they are suspected or known to have been disclosed to unauthorized parties. Should your account become compromised and damage occurs, you will be held accountable. Therefore, it is your responsibility to maintain the confidentiality of your password.
4. After three (3) failed password attempts, you will be locked out of your account.
5. Password-protected screen savers are mandated on all University-owned computers and are set to a maximum timeout of fifteen (15) minutes.
6. Password must not be written down, hidden under a keyboard, or taped to a monitor. Use a password manager that uses encryption if you need to store it.
7. Passwords should not be emailed with usernames.
8. Never save your password in a web form or use the “remember password” feature of applications.
9. Do not use the same password for other non-KSU accounts.
10. IT will never ask you for your password.
11. When IT needs to work on your computer, please make arrangements to be available to type in your password as needed.

Frequency of Password Changes

KSU passwords will expire every 180 days. You will be prompted to change your password with a grace period login notice, which will be sent fourteen (14) days prior to the expiration of your password. Passwords that are not changed before the grace period ends will expire, and you will not be able to access your account.

Password Resets

1. If a user password expires or is typed incorrectly, it can be reset at any time by logging into the password self-service system. The user must be enrolled in the system prior to its use. To log into or enroll in the system please go to: www.kysu.edu/resettool.

2. Passwords may also be reset between 8:00 AM – 4:30 PM by contacting the IT Help Desk. The user may be asked to provide any of the following as identification: the last four digits of his or her Social Security number, his or her 8-digit KSU ID, or picture verification (such as a KSU ID card or driver's license).

3. A temporary password will be set if identification is verified

4. If a password has been compromised, IT will reset the password and enroll the account in multi-factor authentication.

Please note: Remember to log off once you are finished using a computer.

Questions regarding this policy should be directed to the IT Help Desk.

ENFORCEMENT:

Any employee, student, or individual who commits, or refuses to cooperate in the investigation of, a violation of this policy 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.

RELATED POLICIES:

Security Policy

STATUTORY OR REGULATORY REFERENCES:

NIST Special Publication 800-63B