PURPOSE: To provide a secure work environment for data storage area. To ensure that users can only access resources to which they have proper authorization with a login id and a password.

POLICY: It is the policy of Information Technology to assist in changing users’ password and keeping this and each user’s personal information confidential. Passwords will only be administered to the user of the account after proper verification.

1. Passwords should be treated as confidential information and must not be shared. 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.

2. Password protected screen savers are mandated on all University owned computers set to a maximum time out of 15 minutes.

3. KSU passwords will expire every 180 days. You will be prompted with a 14 day grace login notice preceding the expiration of your password. Passwords that are not changed before the grace login period is over will expire and you will not be able to access your account.

4. After 3 tries of failed password attempts, you will be locked out of your account.

Password Resets
1. In the event a user password is typed incorrectly or expires, 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/ksureset.

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 their Social Security number, the 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 the identification is verified.
Password Requirements
1. Passwords are case sensitive.
2. Password requirements are as follows:
   - Passwords must be at least 8 characters in length.
   - Passwords must contain at least one of the following:
     - Upper-case alphabet character (eg. A, C, Q, etc.) or
     - Special character (eg. *, %, !, etc.) or
     - Numeric character (eg. 1,2,4, etc.)
   - Must not contain any part of your account name
   - Cannot match the last 3 passwords

Remember to log off once you are finished using the computer.

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