 <b>SOUTHEAST MISSOURI</b> <b>STATE UNIVERSITY · 1873</b>	<b>BUSINESS  POLICY  AND  PROCEDURE  MANUAL</b>	Date Issued: 09/17	Revision Date: 12/23	Page: 1 of 2
		Classification Code: 10-07		
		Section: INFORMATION TECHNOLOGY		
		Subject: PASSWORD MANAGEMENT		

PURPOSE:

To establish guidelines for the creation, protection, and management of passwords at Southeast Missouri State University.


SCOPE:

This policy applies to all users of Southeast Missouri State University’s information systems and resources, including faculty, staff, students, contractors, and vendors.

GENERAL STATEMENT OF POLICY

Passwords play a crucial role in information security. Poorly chosen passwords may lead to unauthorized access and exploitation of the University’s resources. All users, including contractors and vendors, who have access to University systems are responsible for selecting and securing their passwords.

1. Password Expiration: User-level passwords (e.g., email, web, desktop computer) must be changed as advised by current security guidelines or in case of a suspected security event.
2. Unique System-level Passwords: Users with system-level privileges (e.g., root, enable, Windows Administrator, application administration accounts) must have unique passwords, different from all other accounts they hold.
3. Password Complexity: Users must create strong passwords that meet the following criteria:
  - a. A minimum length of 12 characters.
  - b. A combination of uppercase and lowercase letters, numbers, and special characters.
  - c. Avoidance of easily guessable information (e.g., names, dates, common words)
4. Password Reuse: Passwords must not be used or reused for external accounts or services (e.g., banking, social media).
5. Default Passwords: All vendor-supplied default passwords must be changed before any system can be used in production.
6. Password Sharing: Passwords must not be shared among multiple individuals.
7. Password Storage: Passwords must never be written down or stored online without encryption.

 <b>SOUTHEAST MISSOURI</b> <b>STATE UNIVERSITY · 1873</b>	<b>BUSINESS  POLICY  AND  PROCEDURE  MANUAL</b>	Date Issued: 09/17	Revision Date: 12/23	Page: 2 of 2
				Classification Code: 10-07
		Section: INFORMATION TECHNOLOGY		
		Subject: PASSWORD MANAGEMENT		

8. Reporting Compromised Passwords: Any suspected compromise of account passwords must be reported to the Information Security Officer (ISO) as security incidents.
9. Breach Notification: Upon notification of a breached password, the ISO or a delegate must contact the affected user and request a password change.
10. Password Strength Testing: The ISO or a delegate shall periodically test user passwords for strength.
11. Account Breach Response: In the event of a reported unauthorized account breach, the ISO or a delegate must change the user's password and notify the affected user.
12. Password Reset and Recovery: Users may reset their passwords or perform forgotten password recovery through a secure automated application or by contacting the IT Help Desk.

The Vice President for Finance and Administration shall be responsible for issuing and maintaining operating procedures to implement this policy.