
 SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued:	Revision Date:	Page:
		09/17	12/23	1 of 2
		Classification Code:		
		Section:		
		INFORMATION TECHNOLOGY		
		Subject:		
		IDENTITY AND ACCESS MANAGEMENT		

GENERAL STATEMENT OF POLICY

This policy aims to protect the confidentiality, integrity, and availability of the University's information and network systems. Access to information technology and network systems owned, operated, or leased by Southeast Missouri State University is given for the sole purpose of supporting the University's education, research, and regional service mission. Users of the University's information technology and network systems are responsible for using the systems in a manner consistent with this mission and in compliance with local, state, and federal laws, MORENET regulations, and all policies and procedures of the University.

1. Access to all information technology systems at Southeast Missouri State University shall be controlled using University approved login credentials (e.g., Southeast Key and password). Access from off-campus locations shall be controlled using University approved login credentials and use of a second factor (e.g., MFA, 2FA) including Microsoft Authenticator or SMS text message. Sharing of credentials is strictly prohibited and will be considered a violation of these access controls. All violations of these controls will be subject to disciplinary action up to and including termination of employment.
2. Credential (identity) maintenance for all enrolled or employed members of the Southeast Missouri State University community must be performed using approved online methods, in person, or through other trustworthy mechanisms, as determined by Information Technology.
3. An automated process shall be used to disable or remove a student's system access credentials after graduation or a one-year period of nonattendance
4. Access credentials shall be disabled for repeated misuse.
5. Faculty and staff access shall be disabled or removed upon resignation or termination of employment.
6. Faculty and staff who retire as emeriti may, upon request, be granted continued access to university email services.
7. Character Passwords must have sustainable time complexity as determined by policy 10-07 Password Management.
8. Character passwords must be periodically changed as determined by policy 10-07 Password Management.

 SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 09/17	Revision Date: 03/23	Page: 2 of 2
		Classification Code: 10-01		
		Section: INFORMATION TECHNOLOGY		
		Subject: IDENTITY AND ACCESS MANAGEMENT		

9. Users must keep their passwords private and abide by all University Information Technology policies.
10. Faculty and staff should perform annual security awareness training to ensure they understand their responsibilities in maintaining the security of the University's systems and information.
11. The University shall use a network access control system to validate the identity and appropriateness of those connecting to the campus network.
12. Access to systems and information shall be determined by the user's relationship with the University and the specific information classification. Reference: Business Policy 10-03: Information Technology, Information Security.
13. The Southeast Missouri State University Information Technology department and other relevant personnel will regularly review and update this policy to ensure it remains relevant to evolving technology, threats and regulations.

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