Policy Title:	Multi-Factor Authentication Policy

Governing Body:	Finance and Administration	Policy Number:	
Policy Contact:	Chief Information Officer	Date Revised:	
Custodial Office:	Information Technology	Date Approved:	
Approved By:	President	Next Review:	
Related Policy:	Information Security Policy FAD.040 Password Complexity Requirements and Password Expiration Procedure Acceptable Use of Information Technology Resources Policy FAD.038		

Revision History

Revision Number:	Change:	Date:
1.0	Initial version	**12/11/2017**
1.1	Update to include all employees and clarify language	**4/11/2019**
1.2	Update to include students and clarify language	**Pending**

A. Purpose

The purpose of this policy is to establish standards and requirements for the use of multi-factor authentication to secure access to systems used in the course of university business.

Multi-factor authentication provides an additional level of security to protected accounts, reducing the risks associated with account compromise, phishing, and unauthorized access. Multi-factor authentication is a key component of access controls, is increasingly mandated by regulations, and is required for SOU to meet its security obligations and pass audits.

B. Definitions

SOU Network Account - The primary account that faculty, staff, and students use to access university technology resources. This account is associated with the user's email address with the university (e.g. johndoe@sou.edu) and is the account that gets provisioned at onboarding and deprovisioned at offboarding for all university personnel and students.

Authentication - Authentication is the process of verifying that someone or something is who or what they claim to be. For example, you provide a password to prove that you are who you say you are when accessing a computer system.

Multi-factor Authentication (MFA) - An additional layer of security added to any type of account that requires more than one authentication factor type. Factor types can be:

1. Something you know (e.g. password)
2. Something you have (e.g. physical access to your phone)
3. Something you are (e.g. biometrics, such as a unique fingerprint or iris pattern)

IT Systems - Any equipment, software, or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information.

Single Sign-On (SSO) - A technology that enables the use of a SOU Network Account for authentication across many different systems (e.g. Okta). SSO is convenient and enforces MFA consistently across all the different systems and sites that use it.

Remote Access - Technologies for off-premises access to the university network or information technology systems, such as VPN, Remote Desktop Services, Virtual Desktop Infrastructure, or similar systems.

C. Policy Statement

1. Multi-factor authentication (MFA) is required in the following circumstances:

   A. All employees, including student employees; affiliates; and other non-student individuals with SOU Network Accounts will have MFA enforced immediately upon receiving access.
   B. Students are required to activate multi-factor authentication on their SOU Network Accounts within a grace period after receiving access. MFA will be enabled automatically after the grace period has expired. The grace period shall be determined by the Information Security Office and the deadline will be communicated to students several times during the grace period.
   C. Other IT Systems and accounts beyond the SOU Network Account may require MFA depending on their sensitivity and the security needs of the university. All IT Systems and accounts used in the course of conducting university business may require MFA at the discretion of the Information Security Manager.
   D. All systems that provide Remote Access to the university computing environment or accept interactive connections from the Internet should require MFA before permitting a connection.
   E. Cloud-based or web-hosted systems that are not configured to use Single Sign-On are strongly encouraged to use MFA utilizing their own methods, but those systems may be authorized to operate without MFA at the discretion of the Information Security Manager.

2. Multifactor authentication devices must be safeguarded and must not be shared with others. Lost or stolen devices should be reported immediately to the Information Technology department and, if appropriate, Campus Public Safety. Departments, divisions and/or programs will be charged for replacement multifactor devices, not to include personal devices such as cell phones.

3. The Information Security Manager may consider exceptions to this policy due to technical limitations, system incompatibilities, or accessibility requirements.

> This policy may be revised at any time without notice. All revisions supersede prior policy and are effective immediately upon approval.

D. Policy Consultation

Policy Council.

E. Other Information

The Policy Contact, defined above, will write and maintain the procedures related to this policy and these procedures will be made available within the Custodial Office.