Policy Title:	Multi-Factor Authentication

Governing Body:	Finance and Administration	Policy Number:	FAD.077
Policy Contact:	Chief Information Officer	Date Revised:	
Custodial Office:	Information Technology	Date Approved:	February 19, 2018
Approved By:	President	Next Review:	
Related Policy:	Information Security Policy FAD.040 Password Complexity Requirements and Password Expiration Procedure Computing Resources Acceptable Use Policy FAD.038		

Revision History

Revision Number:	Change:	Date:
	Initial version	February 2018

A. Purpose

The purpose of this policy is to establish standards and requirements for the use of multi-factor authentication with university network accounts.

Multi-factor authentication provides an additional level of security to protected accounts, reducing the risk of account compromise, phishing, and unauthorized access.

B. Definitions

Network Account - This account allows faculty, staff, and students to access university technology resources. These accounts include but are not limited to email, shared network space, and administrative systems.

Multi-factor Authentication - An additional layer of security added to any type of account, requiring extra information or a physical device to login, in addition to a password.

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

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 is required in the following situations:

   A. Any employee or individual providing services in the following departments:
      Business Services
      Enrollment Services
      Human Resources
      Information Technology
      Payroll
      Service Center
   B. Executive staff, including the President, Vice Presidents, and Cabinet members
   C. Any employee, including student employees, who possesses administrative permissions, root access, or system administrator access to university information technology systems and data.
   D. Any employee, including student employees, who modifies or processes employee information, financial information, or tax information.
   E. Any employee or individual using remote access, such as remote desktop services or VPN, for work purposes.
   F. Third-party vendors with university network accounts.
   G. Other systems, purposes, departments, or positions as determined by the Chief Information Officer, a Vice President, or President.

2. Multi-factor authentication is not required but is recommended for all other faculty, staff, and students.

3. Multi-factor 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 and organizations will be charged for lost multi-factor devices, not to include personal devices such as cell phones.

4. The Information Technology department may consider exceptions to this policy due to technical limitations, system incompatibilities, or significant work disruption.

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

D. Policy Consultation

Business Affairs Council, Technology Council, Provost's Advisory Council, Policy Council. Policy was posted on February 7, 2018 for community comment.

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.