Policy Title:	Multi-Factor Authentication Policy

Governing Body:	Finance and Administration	Policy Number:	FAD.077
Policy Contact:	Chief Information Officer	Date Revised:	September 2019
Custodial Office:	Information Technology	Date Approved:	September 27, 2019
Approved By:	President	Next Review:	September 2022
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
1	Updated to include all employees and clarify language	September 2019

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 risks associated with account compromise, phishing, unauthorized access, etc.

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. All employees, student-employees, affiliates and other non-student individuals with university network accounts.

      a. Examples include but are not limited to:
         i. Administrative and Classified Staff
         ii. Faculty
         iii. Third-party vendors with university network accounts
         iv. Emeritus faculty, visiting faculty, fellows

   B. Students are encouraged to adopt multi-factor authentication but are not required to do so unless employed by the university.

   C. Other systems, purposes, departments, or positions as determined by the Chief Information Officer, a Vice President, or the President.

2. 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, programs and/or organizations will be charged for replacement multi-factor devices, not to include personal devices such as cell phones.

3. 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, Cabinet, Executive Council and Policy Council. Policy was posted on September 20, 2019 for community comment.

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.