Title:	Multi-factor Authentication Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	9/4/2018		
Related Policies or Procedures:	EWU 901-02: Appropriate Use of University Resources EWU 203-01: Information Security Policy		

History

Revision Number:	Change:	Date:
1.0	Initial version	9/4/2018
2.0	Updated requirements for usage	1/6/2021

A. Purpose

The purpose of this procedure is to establish standards and requirements for the use of multi-factor authentication with Eastern Washington University 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.

C. Procedure

1. Multi-factor authentication is required in the following situations:

   A. All employees or individuals providing services to the university with university network accounts.
   B. Any student employees that possess administrative permissions, root access, or system administrator access to university information technology systems and data.
   C. Any student employees that modify or process employee information, financial information, or tax information.
   D. Third-party vendors with university network accounts.
   E. 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 student employees.
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, University Police. Departments and organizations will be charged for lost multifactor devices, not to include personal devices such as cell phones.

4. Individuals who are traveling internationally should check with the Director of Risk Management regarding potential export control issues associated with traveling with different types of multi-factor authentication technologies in accordance with EWU Policy 201-10 (Export Control).

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

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