Title:	Password Complexity and Expiration Requirements

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	1/7/2025		
Related Policies or Procedures:	EWU 901-02: Appropriate Use of University Resources EWU 203-01: Information Security Policy NIST SP 800-63-4		

History

Revision Number:	Change:	Date:
1.0	Initial version	10/3/2018
1.1	Password expiry updates	3/18/2021
1.2	Password complexity changes and expiry updates	4/6/2023
1.3	Changes for NIST SP 800-63-4 Compliance	10/14/2024

A. Purpose

This procedure outlines the complexity and expiration requirements for Eastern Washington University network account passwords.

B. Definitions

Generic Account - An account that is intended for shared use.

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.

Special Access Account - This account provides access to specific computer systems, including applications such as Banner, PeopleAdmin, and others.

Resource Account - These are e-mail only or calendar only accounts. They do not permit access to any other systems.

Guest Account – A network or special access account provided on a temporary basis under special circumstances to official guests, vendors, or other affiliates of the university.

C. Procedure

1. Passwords must meet the following requirements:
   - Be unique (never used before)
   - Password IS case sensitive.
   - Be at least 15 characters long.
   - Not include any of the following values: eastern, eagles, 123456, asdfgh, qwerty, changeme, washington, or password
   - Not include a common word or commonly used sequence of characters.
   - Not include part of your name or user name.

2. Passwords known or suspected to be compromised will be deactivated immediately and a change forced.
3. Passwords can be changed once every 24 hours.
4. These requirements apply to all network accounts, generic accounts, resource accounts, and all university systems that manage their own passwords.
5. These requirements will be enforced through network and/or system restrictions.

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