



Information **Technology** Services

## **WSU Authentication Management Standard**

---

Author(s): Keela Ruppenthal  
Bryan Dent


Date: 06/12/2020

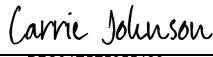
Version: 1.2

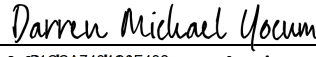
**Revision History**

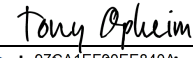
Version No.	Date	Description	Author
1.0	06/12/2020	Initial Release	Keela Ruppenthal Bryan Dent
1.1	06/15/2021	Modified to reflect legacy accounts that are being remediated, the change from 15 to 10-character passwords and an additional authentication strength requirement.	Tony Opheim
1.2	05/03/2022	Modified per Michael Walters and the document authors to update/reflect WSU control objectives for the lockout policy and duration and changes to referenced documents.	Karen Garrett

**Reviewed By:**

DocuSigned by:  
  
 5/3/2022  
 Michael Walters, Interim Chief Information Security Officer Date

DocuSigned by:  
  
 5/3/2022  
 Carrie Johnson, Executive Director, Administrative & Financial Services Date

DocuSigned by:  
  
 5/9/2022  
 Darren Michael Yocum, Assistant Vice Pres, Information Technology Services Date

DocuSigned by:  
  
 5/9/2022  
 Tony Opheim, Associate VP & Deputy CIO Date

**Approvals**

DocuSigned by:  
  
 5/9/2022  
 Sasi Pillay Ph.D., Vice President and CIO Date

## Contents

Revision History .....	ii
Purpose.....	3
Scope .....	3
Statements .....	4
Administrative.....	5
Definitions .....	5
Exceptions .....	5
Review Cycle .....	6
Appendix A: Authentication Requirements.....	7
Appendix B: Glossary .....	9
Acronyms.....	9
Terms.....	9

## Standards References

### Washington State OCIO 141.10.

6.1.1(7), 6.1.2(1) (2) (8) (9)  
(12), 6.2, 6.3

### NIST 800-53 (rev4):

AC (2), AC (6), CM (6), IA (1,  
2, 4, 5, 7, 8)

# Authentication Management

---

## Authentication Management Standard

### Purpose:

Account management and authentication mechanisms are the primary method for protecting WSU Information and IT Resources. This Standard defines requirements for authenticator management, passphrases and authentication mechanisms.

### Scope:

This policy applies to all Institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit Institutional Data.

**Statements:**

1. Information Technology Services shall maintain a centralized authentication platform to ensure that only authorized workforce members (or processes acting on behalf of workforce members) are able to authenticate to WSU systems and applications. This platform will help to ensure that individual workforce members are uniquely authenticated at the time they connect to an information system.
2. Individual unique user IDs and authentication credentials shall be used in combination to access Institutional information resources, such as computers, file servers, electronic mail, printers, mobile devices, cloud-based services, and other network and system infrastructure services that store, process and transmit institutional data, etc.
3. Authenticators utilized for verifying institutional information system users may include passwords, passphrases, passcodes, PINs, biometrics, and digital certificates. PINs and passcodes may be used alone as a single factor only if used on a system that restricts their usability to only local authentications. Authenticator content and the requirements for utilizing authenticators are defined in Appendix A: Authentication Strength Requirements.
4. When utilizing multi-factor authentication to verify that a workforce member is who they indicate to a system, replay-resistant multifactor authentication mechanisms (e.g., one-time passcodes) shall be used. Multi-factor authentication will be required for the following use cases:
  - a. for local access to privileged accounts
  - b. for network access to privileged accounts
  - c. for network access to privileged Tier-1 accounts such that one of the factors is provided by a device separate from the system gaining access
  - d. for local access to University Confidential or Regulated data
  - e. for network access to University Confidential or Regulated data
5. Authenticators must not contain the user's name, UserID or any form of their full name. Authenticators must not consist of a single complete dictionary word but can include a passphrase. An authenticator being changed must be significantly different from the previous four passwords. Authenticators that increment (Password1, Password2, Password3 ...) are not considered significantly different.
6. Passwords should be set to a unique value per user that must be changed immediately after first use.
7. Authentication credentials are considered confidential information and shall be cryptographically protected at-rest and in-transit in accordance with [Executive Policy #8, WSU System Data Policies](#).
8. Files and systems that store authentication credentials will be readable only by users with privileged information system user accounts with the appropriate administrative

Deleted:

privileges. Users of privileged administrative accounts are not to have access to clear text authentication credentials.

9. Information systems will be configured to prevent authentication identifiers and authenticator content from being reused in accordance with university authentication policies and standards. See [Appendix A: Authentication Requirements](#).
10. All privileged system accounts that utilize passwords (e.g., system, root, service, application accounts) will have a unique password for each system and the password shall comply with [Appendix A: Authentication Requirements](#).
11. Information systems should be configured to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). All 3<sup>rd</sup> party workforce members shall be uniquely authenticated and shall be granted access only to the appropriate guest networks.
12. All service accounts will have the default password changed prior to information system installation.
13. Before deploying new devices, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
14. The use of a shared or group authenticator is an exception to this policy requires approval through the ITS Control Exception Policy. In the extraordinary case where shared or group authenticators are approved for use, Information System Owners will adopt a formal process for issuing and distributing approved shared or group account authenticators (e.g., passwords) when membership to those accounts change.
15. Legacy accounts (FIDS and Service Accounts) that have an approved remediation plan by appropriate leadership are exempt from this policy.

### **Administrative:**

The Office of the Chief Information Officer is responsible for the administration of, and the enforcement of compliance with this standard.

### **Definitions:**

For further clarification on the terminology and definition of terms used within this document, please refer to this organization's published glossary of terms associated with this document.

### **Exceptions:**

Exceptions to this policy shall be managed and maintained by the Office of the CIO, following the processes outlined by Configuration Management Policy (BPPM 87.30) and the [ITS Exceptions Process](#).

**Review Cycle:**

This standard is to be reviewed every three years or on an as-needed basis due to changes to technology environments, business operations, or regulatory environments.

**Appendix A: Authentication Requirements**

**Authentication Strength Requirements: Single Factor Password/Passphrase**

Account Type	Setting	Local	Network	Remote
<b>User</b>	Minimum Characters	10		
	Complexity	4/4 Character Types: Upper Case, Lower Case, Number, Special Character		
	Password HistoryValue	24 Generations		
	Minimum PasswordAge	1day/24hrs		
	Maximum Password Age	180 Days		
	Lockout Policy	5 Consecutive Invalid Logon Attempts		
	Lockout Duration	15 minutes		
<b>Service</b>	Minimum Characters	15	Prohibited	
	Complexity	4/4 Character Types: Upper Case, Lower Case, Number, Special Character		
	Password History Value	24 Generations		
	Minimum Password Age	1day/24hrs		
	Maximum Password Age	366 Days		
	Lockout Policy	5 Consecutive Failures		
	Lockout Duration	15 minutes		



<b>Privileged</b>	Minimum Characters	15	Prohibited
	Complexity	4/4 Character Types: Upper Case, Lower Case, Number, Special Character	
	Password History Value	24 Generations	
	Minimum Password Age	1day/24hrs	
	Maximum Password Age	60 Days	
	Lockout Policy	5 Consecutive Failures	
	Lockout Duration	Request Unlock	

**Authentication Strength Requirements: PIN/PASS-Codes used with Multi-Factor**

Account Type	Setting	Local
All	Minimum Characters	6 SMS, 5 Voice
	<p>WSU currently supports multiple multi-factor authentication methods for internal use.</p> <p>These methods include:</p> <ul style="list-style-type: none"> <li>• SMS Authentication - To sign in, you must enter a security token that is sent to your mobile device.</li> <li>• Voice Call Authentication - To sign in, you must enter a security token that is generated, then sent to you via phone call from a mobile device or land line phone.</li> <li>• U2F Security Key (FIDO 1.0) - End-users use a U2F compliant security key.</li> <li>• One time password Security Key – End-users use a HOTP or TOTP ITS compliant security Key.</li> </ul>	

## Appendix B: Glossary

### Acronyms

Acronym	Definition
AFS	Administration & Financial Services
CIO	Chief Information Officer
CISO	Chief Information Security Officer
HOTP	Event one-time password
ITS	Information Technology Services
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
SMS	Short Message Service
TOTP	Time-based one-time password
U2F	Universal 2nd Factor
VP	Vice President
WSU	Washington State University

### Terms

Term	Definition
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).
Multi-Factor Authentication	Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is)

Universal 2nd Factor	Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies two-factor authentication (2FA) using specialized Universal Serial Bus (USB) or near-field communication (NFC) devices based on similar security technology found in smart cards.
Workforce Member	Workforce members include, but are not limited to, employees (faculty, staff, and student interns), contractors, vendors, service providers, volunteers, or any others who have or may come into contact with this organization's data, whether in a paid or unpaid capacity.