Information Technology Services

WSU Account and Identity Management Standard

Author(s): Keela Ruppenthall
Bryan Dent

Date: 06/12/2020

Washington State University

Revision History

Version No.	Date	Description	Author
1.0	06/12/2020	Initial Release	Keela Ruppenthall Bryan Dent

Table of Contents

Standards References

Washington State OCIO 141.10.
5.1.3(1), 6.1

NIST 800-53 (rev4):
AC(1,2,5,6), AT(3), CM(5,6), IA(1-5,8), PM(5)

Account and Identity Management

Account and Identity Management Standard

Purpose:

Account and Identity Management is a set of business processes, information and technology for managing and using digital identities to access and utilize WSU information technology resources and data. This standard includes the people, processes, and technology required to provide secure and auditable access to systems and applications

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 system user and device identifiers will be assigned uniquely and will not be reused nor transferred to another user account or device.
2. Information system user accounts/identifiers shall be disabled if they have been inactive for 180 days.
3. System administrators and other users of information system accounts, or roles, requiring privileged access for their job duties will maintain a non-privileged user account as well as a separate administrative, or privileged account, or role. These two accounts should be managed with different and distinct identities and authentication credentials at all times. Non-privileged accounts, or roles, will be used when accessing non-security or non-privileged functions such accessing email, web browsing, or researching information on the internet. (see Tiered Administration Standard; Role-Based Access Control Standard)
4. Users of information system accounts, or roles, with privileged access will follow the principle of least privilege and will only be used for privileged tasks. Privileged user accounts will be established and administered according to Role-Based Access Control Standards. Privileged accounts and role assignments will be monitored on a regular basis and will be removed when they are no longer appropriate or needed. (See Tiered Administration Standard)
5. Access to server/application system functions, source files, configuration files, and their directories will be restricted to authorized system administrators and other users of privileged information system accounts or roles.
6. Information system accounts and identifiers will be authorized and reviewed by the appropriate University area or departmental Data Custodian or management personnel in accordance with this standard and Access Control and Authorization Policies and Standards.

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 ITS Change and Configuration Management Policy and 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:

Acronyms

Acronym	Definition
AFS	Administration & Financial Services
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ITS	Information Technology Services
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
VP	Vice President
WSU	Washington State University

Terms

Term	Definition
Identifiers	Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers.
Privileged Account	An information system account with approved authorizations of a privileged user.
Credential	An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.
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.