Identity and Access Management Framework Policy

University Operations – Information Security

CWU Policy 204-09

Effective: April 14, 2021

Policy Review Date: YEAR

Policy Executive: Chief of Staff

Responsible Office/Unit: Information Services and Security

Policy Statement:

Applicability:

Content:

---

(1) Identity and access management (IAM) is a framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities. IAM provides secure and auditable access to systems and applications, as well as enabling user lifecycle management. The operational improvements and benefits delivered by IAM help advance core business drivers such as:

A. Improve end-user experience, efficiency, security, and control cost

B. Reduce risk

C. Enhance audit and meet regulatory compliance

(2) Policy

A. The purpose of this policy is to define and implement IAM technologies that can be used to initiate, monitor, and manage digital identities and their related access permissions throughout their lifecycle. This is to be done in an automated manner when possible, with consideration for the need to balance the speed and automation of processes with the control that administrators need to monitor and modify access rights, all while looking to increase efficiencies, without compromising security.

B. CWU shall implement and maintain procedural, physical, technical, and regulatory safeguards and controls that are reasonable and appropriate for the level of information security risk. Those safeguards are to include but not limited to the following components:

1. Utilization of credential management tools.

2. Assigning levels of access to individuals or groups through provisioning processes and security policy enforcement.

3. Protecting the data within the system(s) appropriate with its' classification and securing the system itself.

4. Digital identity governance.

5. Reporting and auditing.

6. Allow comprehensive management and authentication of users.

C. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 information security standard shall be used as a guiding standard, in conjunction with the National Institute of Standards and Technology Framework (NIST). All implemented security controls will be commensurate with asset value, aligned with the appropriate compliance requirements, and as may be determined by an internal risk assessment process.

(3) Scope

A. This policy establishes the IAM framework for CWU and applies to all information systems and information resources owned or operated by or on behalf of the university. All employees are responsible for understanding and adhering to this policy.

(4) Responsibilities

A. The Chief Information Officer is responsible for the operation, management, and oversight of the IAM framework, which assigns and manages digital identities for the university.

(5) Policy Maintenance

A. The Chief Information Security Officer shall review and recommend changes to this policy statement at least annually or more frequently as needed to respond to changes within the institution and the regulatory environment.

(6) Implementation

A. Failure by an individual to comply with this policy may result in disciplinary action up to and including termination for employees, contract termination in the case of contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student.

B. The university reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of a violation of the University policies on information security and privacy.

(7) Additional Information

A. For additional resources, further information on this policy statement, or for a definition of any term used in this policy document, please see Security Services website at https://www.cwu.edu/security-services/.

History:

Responsibility: AVP of ISS; Authority: Cabinet/UPAC; Reviewed/Endorsed by: Cabinet/UPAC; Review/Effective Date: 04/14/2021; Approved by: James L. Gaudino, President
Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-70-080, June 2025
Attached Procedure CWUR 7-70-080 as Appendix A, June 2025

Appendix A - Identity and Access Management Framework Procedure

(1) Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities.

(2) Scope

A. This procedure applies to all information systems and information resources owned or operated by or on behalf of the university. All university employees are responsible for adhering to this procedure and the associated policy, CWU 204-09 Identity and Access Management Framework Policy.

(3) Procedure

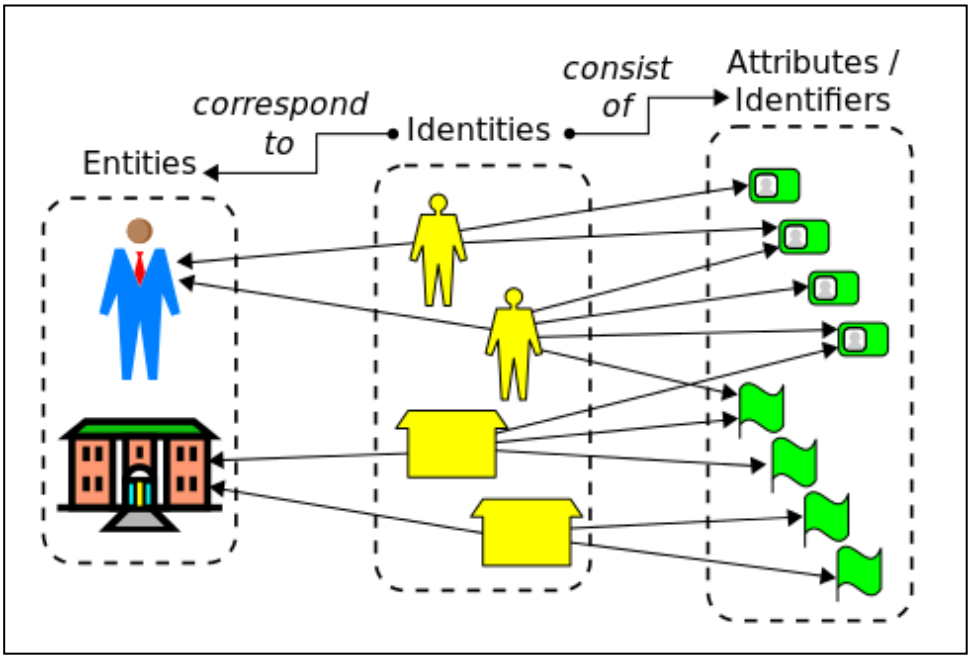
A. IAM is a framework that consists of policies, procedures, and technologies to ensure users have the appropriate and necessary access to resources, services, and locations at the appropriate time. IAM is closely tied to governance, risk, and compliance.

(4) Framework

A. The IAM framework, from a simplified perspective, uses the model described below:

1. CWU shall require a process for establishing levels of confidence in the digital identities used in systems, and a process to revoke them.

2. Each entity should never correspond to more than one digital identity, unless required for clearly defined and documented business or operational reasons (i.e. not convenience). Example of additional digital identities are given below.



(5) Examples

A. For example, the entity Senior VP, has one digital identity that allows logging into MyCWU. Another digital identity of the Senior VP that is connected to the connection card, allows access into certain buildings on campus (i.e. one entity with two identities).

B. Another example is the entity Technical Analyst, who has one digital identity that allows logging into MyCWU and another digital identity that allows privileged access to the network environments (i.e. A-account). The Technical Analyst also has a connection card with access to campus buildings (i.e. one entity with three digital identities).

C. A third example is a student employee who works for the Registrar and has access to student records. This student has a standard user account along with a department position account that grants her/him/them privileged access to the business systems. The student also has a connection card that allows access to her/his/their dormitory (i.e. one entity with three identities).

D. The intent is to keep the number of identities assigned to entities to an absolute minimum.

(6) Provisioning

A. The provisioning process monitors access rights and privileges to ensure the security of university resources and user privacy. As a secondary responsibility, it ensures compliance and minimizes the vulnerability of systems to penetration and abuse. This process for assigning or revoking access rights should include:

1. Requires authorization from the asset/data owner; separate approval for access rights from management may also be appropriate;

2. Verifying that the level of access granted is appropriate and is consistent with other requirements such as segregation of duties;

3. Ensuring that access rights are not activated before authorization procedures are completed;

4. Maintaining a central record of access rights granted to information systems and services;

5. Adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization;

6. Periodically reviewing access rights with owners of the information systems or services.

(7) Control

A. Asset and data owners, as defined in the CWU 204-03 Information Security and Privacy Roles and Responsibilities, should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls consistent with the associated information security risks, or data classification as determined by the CWU 204-04 Data Classification and Usage Policy.

B. A formal, documented, and auditable process for authorization is required.

C. Segregation of access control roles should be used (e.g. access request, access authorization, and access administration).

D. Access is provided on the principle of least-privilege, need-to-know. You are only granted access to the information you need to perform your assigned tasks.

E. Privileged access may require a separate digital identity for an entity, based on the associated information security risks and restrictions determined by the asset/data owner.

F. Where appropriate, role-based access will be used to link access with business roles.

G. Multi-factor authentication is required for all employees.

(8) Review of Access

A. Asset/data owners or their designee should review users' access rights at regular intervals.

B. User access rights should be reviewed and re-allocated when moving from one role to another within the same organization;

C. Authorizations for privileged access rights should be reviewed at more frequent intervals;

D. Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

E. Changes to privileged accounts should be logged for periodic review.

(9) Responsibilities

A. For more information on roles and responsibilities, and definition of terms, refer to CWU 204-03 Information Security and Privacy Roles and Responsibilities.

(10) Procedure Maintenance

A. The Chief Information Security Officer shall review and recommend any change to this procedure statement at least annually or more frequently as needed to respond to changes in the regulatory environment and internal business practices.

(11) Additional Information

A. For additional resources, further information on this policy statement, or for a definition of any term used in this policy document, please see the Security Services website at https://www.cwu.edu/security-services/.