Identity and Access Management Standard			
	Standard No	ITS-2015-S	Rev A
	Owner	IT Security and Compliance	
	Approved by	Sheryl Okuno, Director, IT Security and Compliance	
	Issued 5-2-13 Interim		Revised 2-26-2020
			Page 1 of 17

Table of Contents

1. Purpose

The purpose of this document is to establish standards for Cal State LA's identity and access management (IAM) system. IAM is a process used to facilitate the establishment, management and revocation of user identities and access privileges to University electronic resources. Access to and use of University electronic information resources must be performed in a manner that ensures the confidentiality, integrity and availability of Cal State LA resources and such actions must be conducted in full compliance with federal and state laws, as well as CSU and University policies, standards and practices.

IAM brings together all the information about the authorized IAM users (e.g., student status, employment status, job responsibilities, etc.), enabling centralized control of access to and monitoring of critical systems of the University. Although some University electronic information resources are openly available without authorization (e.g., websites, unencrypted wireless network), access through the IAM system to some systems (e.g., administrative information systems) may only be granted to individuals who have been authorized to have such access and such access may be granted only upon appropriate review and authorization.

The IAM system at Cal State LA is called MyCalStateLA ID. MyCalStateLA ID is a centralized online self-service account offering access to many University systems and services, including the campus high-speed wireless network, MyCalStateLA Portal, e-mail, GET and GETLA, Canvas learning management system, Open Access Labs (OALs), Library resources, MyCalStateLA Tools and others.

In addition, MyCalStateLA ID can grant access to off-campus resources in which Cal State LA is a participant, such as the InCommon Federation and the California State University CSUConnect Federation. InCommon is the federation for U.S. research and education that provides higher education and their commercial and non-profit partners with a common trust framework for access to multiple and diverse online resources. Members of the CSUConnect Federation (CSU students, faculty and staff) have efficient, secure and convenient access to information and services at other participating CSU institutions by using their local campus MyCalStateLA ID credentials.

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
Administrative Procedure 707	**Policy**	**Records Retention, Management and Disposition Program** http://www.calstatela.edu/admfin/administrative-manual-policies-and-procedures This procedure establishes policy for the secure management of University records and the transfer of University records to the State Records Center, the retrieval of stored records and the destruction of obsolete records.
Administrative Procedure 316	**Policy**	**Conditions of Employment** http://www.calstatela.edu/admfin/administrative-manual-policies-and-procedures This document describes requirements and conditions for employment by the University and identifies acceptable documents for verifying identity.
ITS-2006-S	*Standard*	**Information Classification, Handling and Disposal** http://www.calstatela.edu/its/itsecurity/guidelines This standard identifies the three levels of information classification and outlines the best practices for handling and disposing of protected data.
ITS-2008-S	*Standard*	**Password Standards** http://www.calstatela.edu/its/itsecurity/guidelines This standard provides guidance for all users regarding the security and management of passwords.
ITS-1009-G	*Guideline*	**User Guidelines for Separated Employees' Network/E-mail Access** http://www.calstatela.edu/its/itsecurity/guidelines This guideline provides information on network and e-mail access for separated employees.
ITS-1013-G	*Guideline*	**User Guidelines for Data Center/Communications Room Access** http://www.calstatela.edu/its/itsecurity/guidelines This guideline outlines the requirements for obtaining authorized access to data centers and communications rooms.
ITS-1014-G	*Guideline*	**User Guidelines for Access to Administrative Information Systems** http://www.calstatela.edu/its/itsecurity/guidelines This guideline defines the criteria for authorized access to the campus administrative systems (HRM, Financials and GET Student Administration) and outlines the required steps to obtain and maintain administrative systems accounts.

ITS-2007-P	*Procedure*	**Administrative Systems Access Controls and Segregation of Duties Review** http://www.calstatela.edu/its/itsecurity/guidelines This procedure describes the security reports, reviews and remediations required of campus administrative systems to ensure that access controls are consistently implemented and enforced.
InCommon Federation Participant Occupational Practices		**InCommon Federation: Participant Operational Practices** http://www.calstatela.edu/its/incommon/pop/index.php This document outlines the practices of California State University, Los Angeles and the requirements to be maintained as a participant of the InCommon Federation.
CSU Executive Order 1031		**System-wide Records/Information Retention and Disposition Schedules Implementation** https://calstate.policystat.com/policy/6594392/latest/ http://www.calstate.edu/recordsretention This Executive Order provides for the implementation of the California State University (CSU) System wide Records/Information Retention Schedules.
InCommon Federation		**InCommon Federation** http://www.incommonfederation.org/federation/index.html This is the InCommon Federation website.

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3. Entities Affected by These Standards

This standard applies to all University users (e.g., employees, students, and other authorized individuals and organizations) who utilize or manage the Cal State LA IAM system.

4. Definitions

a) Active Directory (AD): Active Directory is a centralized and standardized system that automates network management of user data, security and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

b) Authentication: The process of confirming that a known individual is correctly associated with a given electronic credential (e.g., by use of passwords to confirm correct association with a user or account name). It is a term that is also used to verify the identity of network nodes, programs or messages.

c) Authorization (Network): The function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define access policy.

d) Confidential Information: See Level 1 Confidential Data and Level 2 Internal Use Data. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a security violation has occurred.

e) Data Steward: Individual(s) who have management responsibilities (e.g., planning, policy, etc.) for defined segments of the University data as it relates to their functional operations. Individual(s) with operational responsibility for the physical and electronic security of the data.

f) Department Administrator: Management Personnel Plan (MPP) employee who serves in a leadership role within a unit, department or division. Department administrators generally have a combination of decision-making roles including, but not limited to, financial or budgetary, procurement, personnel, project management, user account approval and signatory authority.

g) Enterprise Active Directory (EAD): One of the components of the Identity and Access Management Program (IAM) at Cal State LA, EAD is a directory service used for authentication and authorization to the centrally managed services deployed University-wide. The University EAD is administered by the IT Infrastructure unit of ITS.

h) Enterprise Systems: Software systems that provide core services used across the University are under the jurisdiction of a centralized information systems department, and on which other applications are often dependent. For example, the Student Administration (SA) System provides the official student record; however, there are often shadow systems that replicate parts of the information maintained in the enterprise system.

i) Federation: An association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.

j) Identification: The assignment of an identifier such as a username for a person or a name for a computer or network device.

k) Identity and Access Management (IAM): The process used to facilitate the establishment, management and revocation of identities and accesses to University electronic resources.

l) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

m) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information many not be released except under certain prescribed conditions.

n) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

o) Segregation of Duties: A security principle that has as its primary objective the prevention of fraud and errors.

p) Separated Employee: Any faculty or staff who severs employment with the University by choice, mutual agreement, end of temporary appointment or non-renewed, automatic resignation (i.e., AWOL), is non-retained or is dismissed for reasons under Education Code 89535.

q) Systems of Record (or University Systems of Record): Administrative systems containing student and employee data that feed directly and automatically into the campus identity management system. Departments that administer systems of record include the Office of Admissions and Recruitment, Registrar's Office, Human Resources Management and the Career Development Center.

5. Standards

The essential functions of identity and access management are identification, authentication, authorization, access management control and accountability.

5.1 Identification

Identification is the act of pre-assigning a unique account credential or identifier (for example, a "username") to an individual such that all entities can be distinguished from each other. The MyCalStateLA ID username is assigned by the Information Technology Services' Infrastructure unit and is not classified as protected data.

Identification control of the IAM system should adhere to the following requirements:

- All users of campus information assets must use only the username assigned by the campus identity management system.
- Insofar as possible, identity information shall be captured from authoritative institutional repositories of information, such as from the Human Resources Management (HRM) system.
- For users whose identity has not been automatically created:
    - Verification of identity must be conducted before identity information is entered into the IAM system.
    - The request must be approved by the authorized individual directly responsible for supervising the requestor's activities and then routed to Information Technology Services.
- Upon receiving alumni status, students shall retain their username, which is permanently associated with the campus identification number (CIN).
- Employees shall not have multiple identities. For example, an individual that is employed by an auxiliary and an academic department of the University shall have one username.

An individual may have two usernames if one is associated with a student CIN and the other with an employee CIN.

5.2 Authentication

Authentication is the act of validating that an entity producing a username (identifier) is the one to which the identifier was assigned. Cal State LA's authentication system provides a highly stable, centrally administered service for use by campus systems that need to authenticate users.

Authentication control of the IAM system should adhere to the following requirements:

- Use of central authentication based on University systems of record, rather than separate authentication systems maintained by individual groups or departments.
- Authentication should be mutual, allowing clients to confirm the identity of the server as well as allowing the server to confirm the identity of the client. This will assist in preventing phishing and man-in-the-middle attacks.
- Authentication should be external to applications so that authentication mechanisms can be updated or changed to reflect changing requirements without requiring significant application development.
- Use of appropriate encryption to protect the privacy of the exchange when electronic credentials are transmitted during authentication.

The IAM system requires a standard Cal State LA password for authentication. Adequate password management is a critical aspect of access control and should include the following:

- Synchronization of password changes between systems.
- Self-service reset of passwords.
- Adherence to campus standards for password security as outlined in *ITS-2008-S Password Standards*.
- Users must not share passwords or log any individuals onto the system who are not authorized to access the system.
- Passwords may not be transmitted without encryption that meets State of California privacy requirements (Information Practices Act, California Civil Code §1798, et. seq.).

5.3 Authorization

Authorization is the act of ensuring that the entity is afforded access only to the services and data required to support allowed tasks. Authorization works hand-in-hand with authentication. Authentication provides the identity of a user, but no information about whether they can access a particular system or service. Authorization determines what level of access that user has, whether they can modify data and whether they can retrieve data.

Authorization control of the IAM system should adhere to the following requirements:

- Push as many applications as possible towards use of workgroups and central authorization systems rather than adding separate authorization systems.
- Adhere to the doctrine of “least privilege.” Users should be granted the lowest level of access necessary to perform job duties or to provide resources needed.

- Authorization to specific services, applications or institutions shall be created without establishing separate identities with each.

5.4 Access Management Control

Access control is a critical information security process that forms the basis of the authority used to determine access to the IAM system server(s) and is limited only to authorized campus affiliates.

Access control of the IAM system server(s) should adhere to the following requirements:

- A formal user access request, review and approval procedure must be in place.
- The access procedure must include both physical (e.g., secured location, environmental conditions, etc.) and logical (e.g., system security, transmissions standards, communications ports, roles, etc.) access controls.
- All IAM servers and network devices must be located in a secure location and physical access control standards must be followed (see *ITS-1013-G User Guidelines for Data Center and Communications Room Access*).
- Access cannot be granted until the user has read and accepted the Statement of Appropriate Use and completed all required Information Security Training (e.g., FERPA certification for employees).
- System backups of the protected data must be physically secured (e.g., in a locked cabinet or stored at a reputable off-site document storage facility).
- System data and files containing Level 1 Confidential Data and Level 2 Internal Use Data must be encrypted.
- Staff authorized for administering and authorizing access control must be clearly identified.
- All changes to user accounts (i.e., account termination, creation and changes to account privileges) must be approved by appropriate campus personnel and formally documented.
- An annual review and formal certification of access control authority must be in place with evidence provided to the director of IT Security and Compliance as part of the campus risk management program.
- Compliance must be assured through logging, auditing and reporting all access, including remote access. If identities and access rights are misaligned, corrective action should be immediately taken to correct the misalignment.
- Orphaned accounts must be terminated immediately.
- Provide mechanisms that allow for the timely provisioning and de-provisioning of access rights. Automate the processes, when possible.

- Regulations (e.g., Sarbanes-Oxley) require a segregation of duties. This is accomplished by continually refining role-based access controls. For example: No one should access the developer environment except developers and their direct managers.

The following access control standards apply to specific University users:

5.4.1 Separated Employees

Access for separated staff is to be revoked the day after the employee's last day of employment. This includes all access permissions to campus information resources assigned to an employee. Department administrators or designees are responsible for submitting separation information into HRM in a prompt manner.

Access for full-time and part-time faculty is to be revoked by the close of business on the published grading deadline or on the last day of employment if the separation occurs after the grading deadline.

5.4.2 Employees on Leave of Absence

Access for employees on a leave of absence may or may not be retained. Determination for continued access is evaluated and granted by Human Resources Management, the office of University Counsel and the appropriate division vice president.

This does not apply to faculty on sabbatical or faculty in FERP.

5.4.3 Part-time Faculty Returning the Following Quarter

Access for part-time faculty who will be returning the following quarter shall be retained.

5.4.4 Faculty on Sabbatical or in FERP

Access for faculty on sabbatical or participating in FERP shall continue.

5.4.5 Emeriti Faculty

Faculty granted emeritus status by the University President shall have access to electronic communications and information as long as they are legally and fiscally feasible.

5.4.6 Contract Employees

Faculty and staff who cease normal employment but are retained on contract with the University (e.g., retired annuitants) shall have their access retained with

approval by the appropriate division vice president and the assistant vice president, Human Resources Management.

5.4.7 Employees Whose Job Duties Have Changed

Employees with access to administrative systems and whose job duties have changed, and this change results in a need to change the related authorization, or no longer require system access, must submit the appropriate Account Modification Request. ITS shall have their access changed by the close of business on the same business day that the request is received.

5.4.8 Employee Suspension of Access for Cause

The vice presidents or the office of University Counsel may request a suspension of access for cause by forwarding a request to the assistant vice president for Human Resources Management. Upon approval by the assistant vice president, HRM will notify the director of IT Security and Compliance of the approved temporary access suspension period. Requests for suspension shall be initiated immediately upon notification. The purpose of the suspension does not require disclosure.

5.4.9 Guest and Shared Accounts

Guests may be granted temporary network guest accounts, which are limited to accessing the campus wired and wireless networks, and the Internet. Guest sponsors must submit *ITS-4818 Network Guest Account Request* and maintain a guest roster that minimally contains guest name, organization, address, phone and campus-assigned guest e-mail address. Guests are never granted access to administrative systems or provided an e-mail account.

There shall be no generic or shared accounts.

5.4.10 Third-party Service Providers

Third-party service providers may be granted temporary network access and/or an e-mail account by submitting *ITS-8828 Third Party Vendor/Consultant Network Access Request*. Service providers may also obtain temporary administrative systems access by submitting the appropriate System Account Request form, available on the ITS forms web page, under Third-party Service Providers, for review and approval.

5.4.11 Campus Auxiliaries

Access for University affiliates is determined on a case-by-case basis following review and approval of submitted system access request forms.

The College of Professional and Global Education may be granted an e-mail account and access to the student administration system (GET) with review and approval.

Associated Students, Inc., University Auxiliary Services, Inc. and the University-Student Union access is limited to e-mail only.

High schools located on University property (LACHSA, MASS) may be granted network and e-mail access only for specific approved purposes, such as providing faculty using University technology classrooms access to equipment and the Internet.

5.4.12 Employee Unions

Access for Union representatives will be provided in accordance with provisions of respective collective bargaining agreements.

5.5 Accountability

Cal State LA must maintain approved security controls and procedures that meet the Chancellor's Office audit requirement to identify inappropriate access and segregation of duty conflicts as well as the maintenance of documents and data.

The processes and supporting systems should be able to provide reports that detail access approvals and reviews, because these are the areas of frequent weakness that are uncovered when auditing an organization's identity and access management process. IAM reporting tools should provide at least the following information:

- Lists of identities and their associated access, both current and historical.
- Critical highlights regarding system access rights.
- Detailed audit logs of user and administrator activities.
- Reports on configuration changes including file and exchange servers.
- The person approving access for specific information.

Documents and data must be retained, managed and destroyed according to *ITS-2006-S Information Classification, Handling, and Disposal*; Administrative Procedure 707 *Records Retention, Management and Disposition Program*; and CSU Executive Order 1031 *System-wide Records/Information Retention and Disposition Schedules Implementation*.

5.6 Enterprise Active Directory Benefits

The Enterprise Active Directory (EAD) is one of the components of the Identity and Access Management Program (IAM) at Cal State LA. EAD is a directory service used

for authentication and authorization to centrally managed services deployed University-wide. A shared EAD services umbrella results in increased efficiency, productivity and satisfaction; enhanced security; higher levels of regulatory compliance; and a reduction in the overall cost of administration.

The following lists some of the specific advantages of a shared EAD services umbrella:

- A reduction in the risk of internal and external attacks because of the reduced number of separate points controlling authorization.
- A reduction in the number of credentials that users must know to perform the action for which they are authorized.
- Improvement in the quality of auditing actions across the University because of the use of persistent identifiers common to all applications.
- A reduction in the denial of service experienced by new members of the University by simplifying and automating provisioning and de-provisioning.
- A constituent's access permissions can be quickly modified as his or her role changes.
- Limits the number of people and offices that can issue credentials and improves procedures for those that do issue credentials.
- Stores the credentials in a secure and centrally managed manner instead of having credentials stored in a variety of systems.
- Consolidates and delivers consistent directory service.
- Manages digital identity data in a way that is person-centric, not system-centric.
- Increases confidence that the credential presented by someone to perform an authorized action is presented by the person to whom the credential was issued.

6. Roles and Responsibilities

Designated University departments and employees must maintain ongoing oversight of the IAM system and related systems.

6.1 Information Technology Services

The campus shall maintain a single IAM system that is managed by the Information Technology Services (ITS) Division. The system maintains the identities, roles and authorities of all users using consistent standards and policies and shall continue to encourage and broaden the use of the IAM system.

6.2 IAM Application Team

The IAM application team serves as the authoritative organizational unit within the University that manages identity information and authentication technology services. The IAM application team consists of the director of IT Infrastructure Services, assistant director of IT Infrastructure Services, director of Enterprise Applications, assistant director of Enterprise Applications. The IAM application team is led by the director of IT Infrastructure Services.

The IAM application team is entrusted by the University with a level of access (privileged accounts) that permits them to make high-level changes to the IAM technology environment including the addition, modification or deletion of users from the applications used in the IAM system. The IAM application team does NOT have responsibility for authenticating the identity of people who are placed into the University systems of record.

IAM application team responsibilities include, but are not limited to:

- Having a unique user identification that identifies the team member (i.e., sysadmin1, sysadmin2 and iamteam1 are unacceptable user ids).
- Fully documenting identity and authentication information.
- Evaluating whether an access request will cause a segregation of duty conflict. If so, notifying the approver of the problem.
- Monitoring access patterns to detect unusual activity.
- Not sharing system administrator rights or logging any individuals onto the system who are not approved to have those rights or access.
- Encrypting system data and files containing protected data, including system administrator passwords.
- Using standardized protocols, formats and software.
- Advising the associate vice president for Information Technology Services of any IAM system activity related to accessing Levels 1 or 2 protected data or modifications to the IAM systems including the introduction of new applications.

6.3 Associate Vice President for Information Technology Services and Chief Information Officer

The associate vice president for Information Technology Services and chief information officer, or designee, should perform the following steps:

- Review the list of users with privileged access to the IAM system quarterly.
- Review all reported incidents of IAM system activity related to accessing Levels 1 or 2 protected data.
- Review and approve any modifications to the IAM system including the introductions of new applications.

6.4 Department Administrators

Department administrators or designees are responsible for the following:

- Maintaining ongoing oversight of access controls to the IAM system to ensure that users granted access remain compliant with appropriate access.
- Reviewing the IAM access granted to their direct reports and identifying and revoking potentially inappropriate access.
- Promptly submitting employee separations to Human Resources Management.
- Submitting the appropriate Account Modification Request when employee's system access requirements change due to new, modified or discontinued job responsibilities, or inter- or intra-division transfers.

6.5 Department Administrators Managing University Systems of Record

Departments responsible to entering or removing student or employee data into or from the University systems of record that feed data to the IAM system have additional responsibilities beyond those cited in section 6.4. These departments include Human Resources Management, Office of Admissions and Recruitment, Registrar's Office and the Career Development Center. The additional responsibilities include:

- Validating the identity of individuals based on approved validation documents (e.g., driver's license, state issued identification with photograph, etc.) prior to activating the applicant, student or employee status.
- Promptly inputting new student and employee data so new accounts will be readily available.
- Promptly removing or modifying student and employee data when notified to do so to ensure student and employee access is removed immediately.

Department administrators and/or data stewards of University systems of record are responsible for complying with all requirements outlined in *ITS-1014-G User Guidelines for Access to Administrative Information Systems*.

6.6 Student Health Center

Assignment of generic accounts to certain personnel on the temporary basis is essential to prevent delays in the Student Health Center services and functions. In consideration of the strict Health Insurance Portability and Accountability Act (HIPAA) requirements to which the Student Health Center must comply, the center is approved to utilize a set of generic accounts to accommodate these personnel. Access to these accounts is managed internally by the Student Health Center security officer.

7. Contacts

a. For questions regarding general information technology security, contact IT Security and Compliance at ITSecurity@calstatela.edu.
b. For technical assistance contact the ITS Help Desk at 3-6170.
c. For questions regarding specific department procedures, contact the department administrator.
d. For questions regarding specific technical procedures, contact the department Information Technology Consultant.

8. Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	**Standards for Privacy of Individually Identifiable Health Information** http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf This is a federal law that protects the privacy of health records.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.8** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that, as amended by SB 1386 (2003), AB 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 residents are involved.