Revision Control

Document Title: IAM Standard
Author: Information Security Officer
File Reference: CPPIAMStandard2013_Final.docx

<table>
<thead>
<tr>
<th>Date</th>
<th>By</th>
<th>Action</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/22/13</td>
<td>Al Arboleda</td>
<td>Initial draft</td>
<td>All</td>
</tr>
<tr>
<td>09/17/13</td>
<td>Al Arboleda</td>
<td>Multiple edit</td>
<td>All</td>
</tr>
<tr>
<td>10/14/13</td>
<td>Al Arboleda</td>
<td>Final Draft</td>
<td>All</td>
</tr>
<tr>
<td>10/17/13</td>
<td>Al Arboleda</td>
<td>Final Revised Draft</td>
<td>All</td>
</tr>
</tbody>
</table>

Review/Approval History

<table>
<thead>
<tr>
<th>Date</th>
<th>By</th>
<th>Action</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/18/13</td>
<td>ISWGC</td>
<td>Approve final draft</td>
<td>All</td>
</tr>
</tbody>
</table>
Identity and Access Management Standard ............................................... 4
Introduction .................................................................................................... 4
Purpose ......................................................................................................... 4
Scope ............................................................................................................. 4
Definitions .................................................................................................... 4
Governance - Administration of IAM Standard ........................................... 5
Identity and Access Management System .................................................. 7
Authorities for Identities, Affiliations and Statuses: ................................... 9
Appendix A: University Affiliations ............................................................ 11
Identity and Access Management Standard

Introduction
Access to and use of electronic information resources must be performed in a manner that ensures the confidentiality, integrity, and availability of university resources and such actions must be conducted in full compliance with federal/state law and CSU policies. Although many electronic information resources are openly available without authorization, access to certain resources may only be granted to individuals who have been authorized to have such access, and such access may be granted only upon appropriate identification and authorization.

Purpose
This standard establishes principles and provisions by which the electronic identities of users and access privileges are managed. Identity and access management is important to ensure that unauthorized electronic access to information, systems, and physical areas is prevented.

Scope
This standard applies to all constituents of Cal Poly Pomona (CPP) who have been granted identifiers for the purpose of using CPP resources and federated online services. Constituents of Cal Poly Pomona include students, staff, faculty, affiliated university organizations, and guests.

Definitions
Directory – The systems and services that comprise the repositories that store the electronic identities, roles and security credentials of all persons affiliated with the university, and the authentication and authorization services that are provided to information systems.

Electronic Identity - An electronic identity is a set of electronic information about a person that identifies that person uniquely. At the Campus, it is at least a single, unique university identifier (Bronco ID), but can include additional attributes such as a single username, password, biometric data, digital photograph, email address, etc.

Federated Identity – Federated identity allows a user’s roles, rights, and privileges to be communicated securely within the US Research and Higher Education community. Cal Poly Pomona is a member of the InCommon Federation. The InCommon Federation is the identity management federation for US research and education, and their sponsored partners. InCommon serves more than 6 million end users through federated identity management.

Identity and Access Management System - Identity and Access Management (IAM) is a set of technologies, processes, and data required to manage the identities of people who have some relationship with the Campus, whether internal or
external, the lifecycle of that relationship and their access privileges to information
and systems.

**Information Authorities** - The stewards for university information assets that are
placed under their control.

**Single Sign-on** - An authentication method whereby a user signs on to one
information system and is consequently automatically signed on to other,
independent information systems.

**Governance - Administration of IAM Standard**
Changes to this standard will be initiated by the Information Security Working
Group, whose co-chair, the Chief Information Security Officer, will then consult with
the necessary levels of management and forums, in order to have standard changes
approved by the Chief Information Officer.

**Identity and Access Management Standard Provisions**
Information stored in the Common Management System (Human Resources and
Student Records) will be used as the System of Record for determining an
individual's identity, role and status. In turn, the role and status will be used for
granting and removing an individual’s access to all online services.

Identity and Access Management is based on the following principles:

1) The university standard will be in line with CSU policy and standards regarding
   Identity and Access control.

2) The university standard will be in line with current Internet 2 eduPerson
   schema specification as used by the InCommon Federation.

3) Access to online services is granted based on the ‘least privilege’ principle.

4) Users will be granted access to resources in a timely manner based on their
   affiliation, role, and/or function.

5) The IAM system provides the tools and infrastructure that enable information
   authorities to manage and audit access rights to their information and systems.
   The management of access remains the responsibility of the information
   authorities. The granting of access privileges is known as authorization.

6) A registry of information authorities and the information and information
   systems for which they are the authorities are established and maintained.
   Information authorities will be required to formally acknowledge and accept
   their responsibilities.

7) Information authorities have specific access management responsibilities in
   relation to the information assets for which they are authorities.
a) Authorities determine who is (or what roles are) granted access to which information and systems and when.
b) Authorities classify data and information under their authority, according to the requirements of the Information Classification and Handling Standard Policy.
c) Authorities manage the process of granting and revoking access to information under their authority.
d) Authorities ensure that access control and privileges are reviewed and audited annually.

8) If information is shared with a third party, a contract must be in place that states they will honor federal/state laws, and applicable CSU policies regarding the protection of information.

9) The university standard will be in line with the InCommon Identity Assurance specification version 1.2 – Bronze level
   a) Credential technology
   b) Credential issuance and management
   c) Authentication process
   d) Identity Information Management
   e) Assertion content
   f) Technical environment

**InCommon Identity Assurance Specification**

In order to maintain our Bronze assurance designation the university must meet all the requirements as defined by the Bronze Identity Assurance profile. Below are the associated relevant Bronze requirements.

1) A person with an affiliation with the Campus will have a single electronic identity. Every person who is a student, employee or affiliate of the Campus is assigned a unique online identity (Bronco ID, and Username). A password is established by the individual for the purpose of authenticating to their assigned identity.

2) An individual’s affiliation (e.g. student, faculty, staff, etc.), role and status at the university govern their access to online services.

3) A person’s affiliation is an attribute of the person’s electronic identity

4) A person may have more than one affiliation or role or function

5) A person’s identity must be adequately validated before the access privileges will be granted by virtue of the role(s) assigned to him/her.

   a) Verification of staff or faculty member’s identity will be conducted before identity information is entered into an authoritative institutional system.

   b) Verification of a student member’s identity will be conducted before a student is issued a university identification card (Bronco Access Card).
c) Identification procedures will require that individuals present a government issued ID containing their picture and an address or record of nationality, e.g., driver's license or passport.

6) The establishment, continuation, and discontinuation of access will be based on an individual’s status at the university (e.g. employed, terminated, registered, alumni, emeritus, etc.).

7) The granting and revocation of access privileges, and all access transactions must be auditable.

8) Identities will be managed through the full lifecycle from identity creation, through provisioning and role changes to ultimate de-provisioning.

9) Appropriate encryption must be used to protect the privacy of the exchange when electronic credentials are transmitted during authentication.

10) The enterprise directory will be managed centrally. Procedures that ensure accurate life cycle management of all users are a necessary component of enterprise directory management. Principles that enable the tracking of individuals through each phase of their affiliation with the university, such as applicant to student, student to faculty or staff, or student to alumni, should be observed.

11) Wherever possible, electronic information about individuals, including guests or sponsored affiliates, in the enterprise directory should be maintained in a manner that ensures the proper electronic verification of identities, non-duplication of electronic identities, facilitates automatic role or group assignment, and facilitates automated provisioning and de-provisioning of services.

Identity and Access Management System

The Chief Information Officer is the information authority for the information contained within the university IAM identity repository and associated IAM components. The Chief Information Officer for the Campus is responsible for the federated online components. The Instructional & Information Division operates the university IAM system under the direction of the Chief Information Officer.

The university identity and access management system includes the following subsystems and components:

- Central authoritative person repository
- Capture identity information from authoritative institutional repositories of information
- Software and processes that generate electronic identities
- All directory systems and services
- All authentication and password management systems
- All software systems that provision and de-provision electronic identities, synchronize identity credentials between systems and codify the rules relating to the above
• Federated identity processes and systems
• User self-service facilities to facilitate individual’s update of personal information and authentication credentials
• Logging, auditing, and reporting tools used to ensure compliance with standard
Authorities for Identities, Affiliations and Statuses:

Identity

**Bronco ID, BroncoName, and Password** - The single university electronic identity. Every person who is a student, staff, faculty, or affiliate of the university is assigned a unique online identity (Bronco ID, and Bronco Name). A password is established by the individual for the purpose of authenticating to their assigned identity. The Chief Information Officer is the Information Authority for the single university electronic identifier.

Major Affiliations

**Students:** The Registrar’s Office is the Information Authority of student records as they are recorded in IAM. As such, they are accountable for ensuring that the information regarding the student’s identity, role, and status at the university are accurate.

**Alumni:** The office of Alumni Affairs is the Information Authority for Alumni records.

**Employees:** The university has multiple offices with Human Resources responsibilities: the Office of Human Resources Management, Foundation Human Resources, ASI Human Resources, and the College of Extended University. These offices are the Information Authorities of employee records. As such, they are accountable for ensuring that the information regarding employee’s identities, roles, and statuses at the university are accurate. Other hiring offices (Auxiliary organizations, Foundation, Academic Planning, Policy & Faculty Affairs, and the employing university departments) are accountable for the timely reporting of changes to roles or statuses of their employees to their respective Human Resource department.

**Faculty Emeriti:** Emeritus status is awarded to retiring faculty members, librarians, coaches and retiring professionals of the related areas constituency of the Academic Senate. Twelve years of university service at the time of retirement is considered the normal measure of eligibility for emeritus status, unless there is objection by the individual or his/her department. Faculty members are identified as emeriti within IAM upon notification from the Office of Human Resources. Faculty Emeriti are individually accountable for reporting to Information & Instructional Technology Services whether they want to retain their electronic identifiers and access to applicable university online services. The Academic Senate, Office of Academic Planning, Policy, and Faculty Affairs, and the Office of the President are the information authorities of the faculty emeriti records. For more information on the emeritus awards process, click on the link below

[http://www.csupomona.edu/~president/emeritus_awards.shtml](http://www.csupomona.edu/~president/emeritus_awards.shtml)
**Staff Emeriti:** Staff emeritus is awarded to retiring staff or management employees who meet certain criteria, including a minimum of 10 years of service to the university, outstanding performance in a position, demonstrated support of university programs, beneficial support of university philosophy, exceptional personal contribution to the university, and active participation in university-wide activities. Individuals are identified as emeriti within IAM upon notification from the Office of Human Resources. Staff Emeriti are individually accountable for reporting to Information & Instructional Technology Services whether they want to retain their electronic identifiers and access to applicable university online services. Staff Council, the Office of Human Resources, and the Office of the President are the information authorities of the staff emeriti records. For more information on the emeritus awards process, click on the link below
http://www.csupomona.edu/~president/emeritus_awards.shtml

**Guest and Sponsored Affiliates:** A university official or designated affiliate sponsor must approve a Guest or Sponsored Affiliate account being granted access within a defined timed period.
## Appendix A: University Affiliations

<table>
<thead>
<tr>
<th>Affiliation Name</th>
<th>Information Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicant</td>
<td>Admissions</td>
</tr>
<tr>
<td>Pending Student</td>
<td>Admissions</td>
</tr>
<tr>
<td>Student</td>
<td>Registrar</td>
</tr>
<tr>
<td>Past Student</td>
<td>Registrar</td>
</tr>
<tr>
<td>Student Staff</td>
<td>Registrar</td>
</tr>
<tr>
<td>CEU Students</td>
<td>CEU Registrar</td>
</tr>
<tr>
<td>Alumni</td>
<td>Alumni Affairs</td>
</tr>
<tr>
<td>Pending Staff</td>
<td>Human Resource Offices</td>
</tr>
<tr>
<td>Staff</td>
<td>Human Resource Offices</td>
</tr>
<tr>
<td>Pending Faculty</td>
<td>Academic Planning, Policy &amp; Faculty Affairs</td>
</tr>
<tr>
<td>Faculty</td>
<td>Academic Planning, Policy &amp; Faculty Affairs</td>
</tr>
<tr>
<td>Instructors</td>
<td>Academic Planning, Policy &amp; Faculty Affairs</td>
</tr>
<tr>
<td>Auxiliary Organization</td>
<td>Multiple (e.g., Foundation, CEU, ASI)</td>
</tr>
<tr>
<td>Sponsored Affiliates</td>
<td>By request</td>
</tr>
<tr>
<td>Faculty Emeriti</td>
<td>Multiple</td>
</tr>
<tr>
<td>Staff Emeriti</td>
<td>Multiple</td>
</tr>
</tbody>
</table>