Pomona College

IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL POLICY

Policy:	Identity Management, Authentication, and Access Control
Policy Owner:	CIO
Change Management	
Original Implementation Date:	3/7/2018
Effective Date:	3/7/2018
Revision Date:	
Approved By:	Executive Staff
Crosswalk	
NIST Cyber Security Framework (CSF)	PR.AC
NIST SP 800-53 Security Controls	AC-2, AC-3, AC-4, AC-5, AC-6, AC-16, AC-17, AC-19, AC-20, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PS-3, PS-4, PS-5, PE -2, PE-3, PE-4, PE-5, PE-6, PE-9, SC-4, SC-7
NIST SP 800-171 Protecting Controlled Unclassified Information	3.1, 3.5, 3.10.1, 3.10.3, 3.10.4, 30.10.5, 3.10.6
Center for Internet Security Critical Security Control	CSC 12, 15, 16
Payment Card Industry Data Security Standard (PCI DSS) v3.2	1.1, 1.2, 1.3, 4.3, 7.1, 7.2, 7.3, 8.7, 8.8, 11.1,
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance in developing and implementing the appropriate protective safeguards to ensure the confidentiality, integrity, and availability of Pomona College assets and information.

POLICY

Identity management, accounts, and access control are paramount to protecting Pomona College's system and requires the implementation of controls and oversight to restrict access appropriately. Pomona College limits access to the system, system components, and associated facilities to authorized users, processes, and devices in support of Pomona College's mission and business functions.

LOGICAL ACCESS MANAGEMENT

ACCOUNT MANAGEMENT

ROLE BASED ACCESS CONTROL

- Pomona College:
  - Maintains role based account types to which individuals are assigned in support of Pomona College mission and business functions
  - Assigns account managers for system accounts
  - Establishes conditions for group and role membership
  - Specifies authorized users of the system, group and role membership, and access authorizations and other attributes for each account
  - Requires approvals by the Head of Human Resources, Dean of the College, Admission, the Office of the Registrar, Dean of Students, or appropriate designees depending upon the role of the user
  - Creates, enables, modifies, disables, and removes system accounts in accordance with Pomona College policies
  - Monitors the use of system accounts for suspicious activity that is indicative of unauthorized access attempts or an attack on the Pomona College system
  - Account managers are notified when:
    - Accounts are subject to legal hold
    - Accounts are no longer required
    - Users are terminated, or transferred
    - Individual system usage or need-to-know changes
  - Authorizes access to the system based upon:
    - A valid access authorization
    - Intended system usage
    - Other attributes as required by Pomona College
  - Annually reviews accounts for compliance with account management requirements
  - Establishes a process for reissuing shared/group account credentials when individuals are removed from the group
- All individuals granted a Pomona College account agree to comply with the following:
  - All eligible individuals are assigned Pomona College system IDs.
  - Individuals are responsible for protecting their account credentials. They should never disclose account credentials under any circumstances. Individuals should take all reasonable precautions, including, but not limited to, password changes and other file protection measures to prevent unauthorized use of the system and software accessible by their accounts. If individuals believe that their account credentials have been compromised, then they should contact ITS as soon as possible.
  - Individuals must respect the privacy of others and the integrity of Pomona College's computing and network systems, and must comply with the Acceptable Use Policy.
  - Pomona College faculty and staff must use a non-forwarding, Pomona College email account for work-related correspondence. Work related correspondence should not be auto-forwarded to non-Pomona College accounts.
  - Work for Pomona College is to be largely completed and ultimately stored on Pomona College-owned or managed services.

        - The Pomona College ITS website contains a complete list of owned or managed tools and services.
    - Pomona College will make reasonable efforts to maintain the confidentiality, integrity, and availability of files stored on Pomona College hardware. Pomona College is, however, not liable for the inadvertent or unavoidable loss or disclosure of the contents, for disclosure resulting from the unlawful acts of others, or for disclosure required by law.
- Pomona College employs automated mechanisms to support the management of system accounts:
    - After a period of time, defined by the user's role, the Pomona College system will lock the use session with a pattern-hiding display to prevent access or viewing by unauthorized individuals.
    - After a period of time, defined by the user's role, the Pomona College system will terminate the user's session to prevent access or viewing by unauthorized individuals.
- The Pomona College system disables temporary[1] and emergency accounts[2] (if applicable) after a period of no more than 24-hours.
- User accounts provided by Pomona College serve to individually identify users of Pomona College technology systems and resources, such as email, network resources, remote access, web-based services, and other electronic resources. Pomona College account creation is authorized by the Head of Human Resources, Admissions, Dean of the College, or the office of the Registrar depending upon the role of the user. Individuals eligible for Pomona College accounts include
    - Pomona College full and part-time faculty and staff
    - Currently-admitted students
    - Trustees
    - Alumni
    - Faculty Emeriti
    - Summer Scholars
    - Currently enrolled cross-registered students
    - Non-Pomona student employees
    - Temporary workers while working at the College (at the discretion of the division head and Human Resources management)
    - Faculty or staff on official sabbaticals or leaves of absence
    - Librarians of the Claremont Colleges
- Terminated staff, voluntary (including retired) and involuntary, and partners of staff or faculty with no other affiliation with the College are generally not eligible for a Pomona College account, sponsored, temporary, or otherwise.
- The system logs account creation, modification, enabling, disabling, and removal actions.
    - Where technically feasible, the system notifies Pomona College ITS personnel of anomalous events.

NON-STANDARD ACCOUNTS

- For otherwise non-eligible individuals, a sponsored account may be requested via a sponsoring department or other appropriate individual, and it must be approved by the Chief Information Officer (CIO) of Information Technology Services (ITS), or designee. Sponsored accounts are, by default, active for a maximum of one year, unless renewed.

[1] Pomona College establishes temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

[2] Pomona College establishes emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes

  - Requests for sponsored accounts should be submitted in writing to the Office of the Dean of the College or to the Head of Human Resources (HR). Please include the specific need for the account in the request.
- Conference and event organizers may request guest accounts for their participants. Guest account requests need to be submitted to the Pomona College ITS Service Desk and include the specific need for the guest account(s). Conference and event organizers must accept full responsibility for all activities that occur with any quest accounts they request.

ACCESS TERMINATION

- Accounts identified as no longer having any business function are deactivated. Unless an explicit exemption is granted (e.g., prior arrangement with the appropriate Vice President or HR management, and approved by the CIO or ITS designee), Pomona College staff accounts are deactivated within one (1) business day of a staff member's effective termination date.
- In the event of involuntary termination, deactivation will occur immediately at the time pre-arranged with HR management and the respective Department Head.
- At the time of access termination, for faculty and staff accounts, Pomona College HR conducts exit interviews that include information security, and all Pomona College property and assets are collected from the terminated individual
- In the event of the death of a Pomona College Student, Faculty, or Staff member Pomona College will deactivate the deceased individual's account
  - Upon request of authorized individuals, including but not limited to next of kin, law enforcement, and/or court order, the contents of the deceased individuals account will be made available to the appropriate parties
  - Where appropriate, Pomona College reserves the right to curate the contents of the individual's account prior to release
- Unless an explicit exemption is granted (e.g., retirement or prior arrangement with the academic dean's office, and approved by the CIO or ITS designee), faculty access is deactivated 180 days following the faculty member's effective termination date
- Graduating Pomona College students will have their accounts migrated to Alumni status the first business week in December following the date of separation from the College.
- Students who transfer, withdraw, or otherwise do not return to Pomona College (with the exception of Students on leave) will have their access deactivated either:
  - Within one (1) business day of when records are updated by the Registrar's office, or
  - One (1) semester after the date they last attended classes. Students will generally be given at least one month of notice before account deactivation.
- Students on approved leave will retain access to their accounts for the duration of the leave. The Registrar's policies determine the leave status and when the account status is changed to deactivated.
- Deactivated accounts are deleted per the Data Retention section of the Security Operations policy
- Accounts, both active and disabled, are monitored for anomalous activity, and in the event anomalous activity is detected, appropriate measures will be taken.

PERSONNEL TRANSFER

- Pomona College:

  - Reviews and confirms ongoing operational need for current logical and physical access authorizations to the Pomona College systems and facilities when individuals are reassigned or transferred to other positions
  - Initiates transfer within 24-hours following the formal transfer action
  - Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer
  - Notifies the Security Official, or designee, within 48-hours

PASSWORDS

- Passwords are used to authenticate accounts, and should therefore only be known to the individual whose identity is tied to the account. Individuals need to take necessary steps to ensure they maintain the secrecy of their passwords. Methods of ensuring password secrecy include:
  - Never sharing passwords
  - Never writing down passwords
  - Using a secure password management tool
- Access to user account IDs and/or passwords may not be loaned or sold, and any suspected compromise of password security should be immediately reported to the Pomona College ITS Service Desk.
- Passwords need to be of sufficient strength that it would be impractical for an attacker to guess or otherwise discover the correct secret value, while still maintaining adequate usability for the user. Pomona College requires the following:
  - Passwords shall be at least eight (8) characters in length
    - It is recommended that users make their passwords as long as possible, within reason. A 16-character password or passphrase is currently sufficient to both protect user accounts and be functionally memorized.
  - Pomona College may disallow some password choices based upon their appearance on a list of prohibited passwords, which may include but is not limited to:
    - Passwords obtained from previous data breaches
    - Dictionary words
    - Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
    - Context specific words, such as the name of the service, the username, and derivatives thereof
  - Passwords are not required to be changed periodically
  - Passwords are required to be changed if the user requests a change or there is evidence of a compromise of the password
  - Passwords should be stored in a manner that is resistant to offline attacks
- The Pomona College system will limit the number of unsuccessful authentication attempts.
- If an individual’s password becomes compromised, or is suspected to be compromised, they are to report this immediately to the Pomona College ITS Service desk. The ITS Service Desk will then revoke the password and initiate a password reset process for the affected individual(s).
- Pomona College ITS will never ask a user for his/her password. If there is ever a need by ITS for a user’s password, then the user will be asked to be present.
  - If the user is unavailable, then Pomona College ITS will reset the password.
- Pomona College manages its system authenticators (passwords) by:
  - Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator

  - Establishing initial password content for passwords defined by Pomona College
  - Ensuring that passwords have sufficient strength of mechanism for their intended use
  - Establishing and implementing administrative procedures for initial password distribution, for lost/compromised or damaged passwords, and for revoking passwords
  - Changing default content of passwords prior to system installation
  - Establishing reuse conditions for passwords in the event a password is ever changed
  - Protecting password content from unauthorized disclosure and modification
  - Requiring individuals to take, and having devices implement, specific security safeguards to protect passwords
  - Changing passwords for group/role accounts when membership to those accounts changes
- Pomona College's system obscures feedback of password information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.
  - Pomona College's system offers an option to display the password until it is entered.
- The Pomona College system employs mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

MULTI-FACTOR AUTHENTICATION

- Pomona College requires the use of multi-factor authentication for:
  - Network access for privileged accounts (e.g. administrator, root, sudo)
  - Local access to privileged access accounts
  - Remote access to both privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system on which the user is gaining remote access
  - Authentication to Pomona College's Single Sign On (SSO) through the Central Authentication Service (CAS), where technically feasible

ACCESS CONTROL FOR MOBILE DEVICES

- Pomona College:
  - Has established usage restrictions, configuration requirements, connection requirements, and implementation guidance for Pomona College-controlled mobile devices
  - Authorizes the connection of other mobile devices to the Pomona College system

WIRELESS ACCESS

- Pomona College:
  - Has established usage restrictions, configuration/connection requirements, and implementation guidance for wireless access
  - Authorizes wireless access to the system prior to allowing such connections
- The Pomona College system protects wireless access to the system via user and/or device authentication and encryption.
- Pomona College identifies and explicitly authorizes users who are allowed to independently configure wireless networking capabilities.

USE OF EXTERNAL SYSTEMS

- Consistent with any trust relationship established by Pomona College with other organizations owning, operating, and/or maintaining external systems, Pomona College has established terms and conditions allowing authorized individuals to:
  - Access the Pomona College system from external systems
  - Process, store, or transmit Pomona College-controlled information using external systems
- Pomona College permits authorized specific individuals to use an external system to access the Pomona College system, or to process, store, or transmit Pomona College-controlled information only when Pomona College:
  - Verifies the implementation of required security controls on the external system as specified by Pomona College policy; or
  - Retains approved system connection or processing agreements with the organization hosting the external system
- Pomona College discourages the use of Pomona College-controlled portable storage devices (e.g., Pomona College-issued smartphones and/or laptops) by authorized individuals on untrusted, public external systems

PHYSICICAL ACCESS MANAGEMENT

- Physical access to critical Pomona College assets is managed and protected. In order to manage this physical access, Pomona College maintains a list of authorized individuals, and the corresponding facilities to which they are allowed access.
  - This list is reviewed and Pomona College updates/removes individuals from this list when access needs change, or are no longer required
  - Pomona College issues authorization credentials for facilities access
- Pomona College controls physical access to its critical system and transmission lines within Pomona College facilities by:
  - Verifying individual access authorizations before granting access to the facility
  - Controlling ingress/egress to the facility using physical access control systems
  - Maintaining physical access audit logs for specified sensitive entry/exit points
  - Providing safeguards to control access to areas within the facility officially designated as publicly accessible
  - Securing keys, combinations, and other physical access devices
  - Inventorying physical access devices quarterly
  - Changing combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated
- Pomona College controls physical access to system Output Devices[3] to prevent unauthorized individuals from obtaining the output.
- Pomona College will employ privacy screens on workstation monitors where deemed appropriate to prevent unauthorized individuals from compromising the confidentiality of sensitive information.
- Pomona College monitors physical access to facilities where the critical systems reside in order to detect and respond to physical security incidents. Physical access monitoring may include:
  - Intrusion alarms
  - Automated intrusion recognition
  - Video surveillance

[3] Output devices include but are not limited to: monitors, printers, copiers, scanners, fax machines, and audio devices.

    - Monitoring of physical access to systems in addition to monitoring physical access to the facility in which the systems reside
- Pomona College:
    - Authorizes visitors before entering specific controlled areas[4]
    - Escorts visitors and monitors visitor activity within defined specific controlled areas and facilities
    - Issues visitors a badge or other identification that expires and that visibly distinguishes them from Pomona College Faculty, Staff, and Students
        - Visitors are asked to turn in their badge or identification before leaving the defined sensitive area or facility
    - Maintains visitor access records to defined sensitive areas and facilities, including, but not limited to the facility where the system resides for a minimum of three (3) months.
        - Access records are reviewed quarterly

REMOTE ACCESS MANAGMENT

- Pomona College has established and documented usage restrictions, configuration requirements, connection requirements, and implementation guidance for the types of remote access allowed.
- Remote access to the Pomona College system is first authorized before any such remote connections are allowed.
    - Authorized individuals are subject to the requirements of Pomona College's Appropriate Use Policy when accessing the system remotely
- The Pomona College system monitors and controls remote access methods.
    - Automated monitoring and control of remote access allows Pomona College to detect security events and ensures ongoing compliance with remote access policies
- The Pomona College system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
- Remote access is routed through specific managed network access control points.
    - Limiting the number of access control points for remote access reduces the attack surface of Pomona College
- Pomona College authorizes the execution of privileged commands, and access to security-related information via remote access only for the purpose of providing remote support.

ACCESS PERMISSION AND AUTHORIZATION MANAGEMENT

- Pomona College:
    - Screens staff prior to authorizing access to the system
    - Screens faculty as part of the hiring process
    - Student screening is part of the admissions process
- Pomona College:
    - Separates duties between:
        - Individuals responsible for mission functions and system support functions
        - Individuals conducting system support functions and system management, programming, configuration management, quality assurance, and testing
        - Individuals administering access control functions and those who administer audit functions

[4] Controlled areas are those areas of the College where confidential information and/or systems reside, i.e. the ITS data center and ITS office spaces behind the RFID controlled doors.

  - Pomona College documents the separation of duties of individuals
  - Defines system access authorizations to support separation of duties
- Pomona College employs the principle of least privilege, allowing only authorized access for users, or processes acting on behalf of users, which are necessary to accomplish assigned tasks in accordance with Pomona College mission and business functions.
- Pomona College explicitly authorizes individuals access to:
  - Establish system accounts
  - Configure access authorizations
  - Set events to be audited
  - Configure intrusion detection parameters
- The Pomona College system prevents unauthorized and unintended information transfer via shared system resources
- Pomona College requires that users who possess system privileged accounts, use non-privileged accounts when performing functions that do not require escalated privilege.
- Pomona College restricts privileged accounts on the system to specific roles within the College.
- The Pomona College system prevents non-privileged users from executing privileged functions that include, but are not limited to disabling, circumventing, or altering implemented security safeguards and countermeasures.

NETWORK INTEGRITY

- The Pomona College system:
  - Implements subnetworks for publically accessible system components that are separated from internal organizational networks
  - Connects to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the Pomona College security architecture
- Pomona College limits the number of external network connections to the system.
- Pomona College:
  - Implements a managed interface for each external telecommunication service
  - Establishes a traffic flow policy for each managed interface
  - Protects the confidentiality and integrity of the information being transmitted across each interface
  - Documents each exception to the traffic flow policy with a supporting mission or business need
  - Reviews exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit need
- The system, at managed interfaces, denies network communications traffic by default and allows network communications traffic by exception (deny all, permit by exception).
- The Pomona College system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicative via some other connection to resources in external networks (i.e., disable split-tunneling).