SYSTEMS ASSET MANAGEMENT POLICY

Policy:	Asset Management
Policy Owner:	CIO
Change Management	
Original Implementation Date:	7/1/2017
Effective Date:	7/1/2017
Revision Date:	
Approved By:	Executive Staff
Crosswalk	
NIST Cyber Security Framework (CSF)	ID.AM
NIST SP 800-53 Security Controls	AC-4, AC-20, CM-8, CP-2, PS-7, PL-8, PM-11, RA-2, CA-3, CA-9, SA-9, SA-14
NIST SP 800-171 Protecting Controlled Unclassified Information	3.4.1, 3.4.2
Center for Internet Security Critical Security Control	CSC 1, CSC 2
Payment Card Industry Data Security Standard (PCI DSS) v3.2	
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance in identifying and gaining an understanding of the components of the institution that make up its information security system and thereby enable Pomona College to manage cybersecurity risk to systems, assets, data, and capabilities.

POLICY

In order for Pomona College leadership to make informed, business-driven decisions regarding computing assets, they must first know what assets exist, and the status of those assets. This information provides Pomona College visibility into license utilization, software support costs, unauthorized devices, vulnerabilities, threats, and compliance posture. IT assets include items such as servers, desktops, laptops, and network devices, as well as software, applications, programs and logical processes. Pomona College data, students, faculty, staff, devices, systems, and facilities that enable the organization to achieve educational, business, and operational purposes are identified and managed. The management of these assets is consistent with their relative importance to Pomona College educational, business, and operational objectives as well as Pomona College's overall risk strategy.

PHYSICAL ASSET INVENTORY

- Pomona College maintains an inventory of physical system components that:
  - Accurately reflect the Pomona College system
  - Includes all physical components within the authorization boundary of the Pomona College system
  - Is at a level of detail necessary for appropriate tracking and status reporting of assets
  - Includes hardware inventory specifications (e.g. manufacturer, device type, model, serial number, physical location), component owners, machine names, and network addresses
- The inventory of physical devices is updated whenever:
  - Physical system components are installed
  - Physical system components are removed
  - The system is updated
- Pomona College employs automated mechanisms to detect the presence of unauthorized hardware within its system. Whenever unauthorized hardware is detected, network access is disabled and Pomona College Information Technology Services (ITS) is notified.
- Pomona College verifies that all components within the authorization boundary of the Pomona College system are not duplicated in other system component inventories.
- Pomona College periodically reviews and updates the Physical Asset Inventory.

SOFTWARE ASSET INVENTORY

- Pomona College maintains an inventory of logical system components that:
  - Accurately reflect the Pomona College system
  - Includes all software components within the authorization boundary of the Pomona College system
  - Is at a level of detail necessary for appropriate tracking and status reporting of assets
  - Includes items such as software license number and component owners
- The inventory of software is updated whenever:
  - Logical system components are installed
  - Logical system components are removed
  - The system is updated
- Pomona College employs automated mechanisms to detect the presence of unauthorized software and firmware within its system:
  - Whenever unauthorized logical components are detected the component is isolated and Pomona College Information Technology Services (ITS) is notified
- Pomona College verifies that all components within the authorization boundary of the Pomona College system are not duplicated in other system component inventories.
- Pomona College periodically reviews and updates the Software Asset Inventory.

ORGANIZATIONAL DATAFLOW MAPPING

- Pomona College maintains and authorizes internal connections of components to the system.
- Pomona College documents the internal connection characteristics, security requirements, and nature of the information communicated.

INFORMATION SECURITY ARCHITECTURE

- Pomona College:
  - Maintains an information security architecture for the Pomona College system that:
    - Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of Pomona College information
    - Describes how the information security architecture is integrated into and supports the enterprise architecture
    - Describes any information security assumptions about, and dependencies on, external services
  - Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture
  - Ensures that planned information security architecture changes are reflected in the security plan and Pomona College procurements and acquisitions
- Pomona College's security architecture uses a defense-in-depth approach that:
  - Allocates appropriate security safeguards to Pomona College assets; and
  - Ensures that allocated security safeguards operate in a coordinated and mutually reinforcing manner

EXTERNAL SYSTEMS

- External systems utilized by Pomona College are identified and catalogued.
  - Pomona College authorizes connections from its system to other systems through the use of Interconnection Security Agreements
  - The documentation for each interconnection includes:
    - Interface characteristics
    - Security requirements
    - The nature of the information communicated
  - Pomona College reviews and updates its Interconnection Security Agreements annually, or upon a significant change to the Pomona College system or to the external systems.
- Pomona College requires that providers of external system services comply with its information security requirements, and employ the necessary controls to comply with applicable state and federal law.
  - Pomona College monitors external system service providers' security control compliance on an ongoing basis.
  - Pomona College requires external system services to identify the functions, ports, protocols, and other services required for the use of such services.
- Pomona College establishes terms and conditions with approved external systems allowing authorized faculty, staff, or students to access these external systems, and to process, store or transmit Pomona College-controlled information using approved external systems.

- Pomona College employs a permit-by-exception policy for allowing Pomona College system components to connect to external systems.
- Pomona College permits authorized individuals to use external systems to access the Pomona College system or to process, store, or transmit Pomona College information only when:
  - Pomona College verifies the implementation of required security controls on the external system as specified by Pomona College policy; or
  - Pomona College retains approved system connections or processing agreements with the third-party hosting the external system.
- Pomona College restricts the use of Pomona College-controlled portable devices by authorized individuals on external systems.

SECURITY CATEGORIZATION

- Pomona College:
  - Categorizes information, the system, and its components in accordance with applicable laws, regulations, policies, and guidance
  - Documents the security categorization results, and their supporting rationale, in the Pomona College information security plan
  - Ensures that the Security Official reviews and approves of security categorization decisions.
- Pomona College's security categorization schema follows a three-tier methodology:
  - Public – Unauthorized use, disclosure, alteration, or destruction of Public information will result in little or no risk to Pomona College.
  - Proprietary – Unauthorized use, disclosure, alteration, or destruction of Proprietary information could result in moderate risk to Pomona College. By default, all institutional data that is not explicitly categorized as Confidential or Public is treated as Proprietary.
  - Confidential - Unauthorized use, disclosure, alteration, or destruction of Confidential information could result in significant risk to Pomona College. Examples of Confidential information include but are not limited to Controlled Unclassified Information (CUI)[1].

RESOURCE PRIORITIZATION

- Pomona College assets and resources, including but not limited to hardware, devices, data, and software, are prioritized based on their categorization, criticality, and business value.
  - Critical assets are identified by Pomona College so that additional safeguards and countermeasures are employed to help ensure that Pomona College mission functions can continue during contingency operations.
- A criticality analysis is a key tenant of risk management and informs the prioritization of protection activities for Pomona College.

ASSET ROLES AND RESPONSIBILITIES

[1]Controlled Unclassified Information - https://www.archives.gov/cui/registry/category-list

- Pomona College establishes asset management roles and responsibilities for faculty, staff, and third-party stakeholders, including (but not limited to) vendors, suppliers, customers, and partners.