



SYSTEMS ASSET MANAGEMENT POLICY





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