

TECHNOLOGY ACQUISITION AND DISPOSITION POLICY

Policy:	Technology Acquisition and Disposition
Policy Owner:	CIO
Change Management	
Original Implementation Date:	3/7/2018
Effective Date:	3/7/2018
Revision Date:	
Approved By:	Executive Staff
Crosswalk	
NIST SP 800-53 Security Controls	SA-4, SA-5, SA-9
Center for Internet Security Critical Security Control	10
Payment Card Industry Data Security Standard (PCI DSS) v3.2	2.1, 2.5, 2.6
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance to develop and implement the appropriate activities with regards to the acquisition, and eventual disposition of information technology assets, Pomona College system components, and third-party services.

POLICY

Pomona College exercises due diligence and due care when engaging in the acquisition of information technology assets, including but not limited to, Pomona College system components, hardware, software, and third-party services. Pomona College recognizes that information technology assets have a limited useful lifespan and will designate appropriate End-of-Life (EoL) for information technology assets.

ACQUISITION PROCESS

- ❖ Pomona College includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the Pomona College system, system components, or system service in accordance with applicable Federal and State laws, regulations, and the Pomona College educational mission and business needs
 - Security functional requirements
 - Security strength requirements
 - Security assurance requirements
 - Security-related documentation requirements
 - Requirements for protecting security-related documentation

- Description of the system development environment and environment(s) in which the system is intended to operate
- Acceptance criteria
- ❖ Pomona College requires the developer of the Pomona College system, system components, or information system service to provide design and implementation information for the security controls to be employed that includes (where appropriate):
 - Security-related external system interfaces
 - High-level design
 - Low-level design
 - Source code
 - Hardware schematics
- ❖ Pomona College requires the developer of the Pomona College system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for Pomona College use.

INFORMATION SYSTEM DOCUMENTATION

- ❖ Pomona College:
 - Obtains administrator documentation for the Pomona College system, system component, or information system service that describes:
 - Secure configuration, installation, and operation of the system, component, or services
 - Effective use and maintenance of security functions and mechanisms
 - Known vulnerabilities regarding configuration and use of administrative, or privileged, functions
 - Obtains user documentation for the Pomona College system, system component, or information system service that describes:
 - User-accessible security functions and mechanisms, and how to effectively use those security functions and mechanisms
 - Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner
 - User responsibilities in maintaining the security of the system, component or service
 - Documents attempts to obtain the Pomona College system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.
 - This documentation includes the responses to the attempts
 - Protects documentation as required, in accordance with the Pomona College risk management strategy
 - Distributes documentation to appropriate roles and individuals

EXTERNAL INFORMATION SYSTEM SERVICES

- ❖ Pomona College:
 - Requires that providers of external information system services comply with Pomona College security requirements and employ reasonable and appropriate security controls in accordance with Federal and State laws, and regulations
 - Defines user roles and responsibilities with regard to external information system services
 - Employs reasonable and appropriate measures to monitor security control compliance by external service providers on an ongoing basis

- Requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services

END OF LIFE

- ❖ Pomona College designates a defined End-of-Life (EoL) period for all Pomona College system components, and hardware
- ❖ Upon reaching EoL Pomona College system components and hardware are to be replaced with new information technology assets
- ❖ Upon reaching EoL Pomona College system components and hardware are to be disposed of in accordance with Pomona College policy¹

¹ See Pomona College Security Operations policy, Data Destruction