SYSTEMS GOVERNANCE POLICY

Policy:	Governance Environment
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.GV
NIST SP 800-53 Security Controls	AC-1, AU-1, AT-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PS-1, PS-7, PE-1, PL-1, PM-1, PM-9, PM-11, RA-1, CA-1, SC-1, SI-1, SA-1
NIST SP 800-171 Protecting Controlled Unclassified Information	3.1 – 3.14
Center for Internet Security Critical Security Control	1-20
Payment Card Industry Data Security Standard (PCI DSS) v3.2	12
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

Pomona College develops, maintains, and disseminates an information security program that includes information security policies and procedures. These policies, procedures, and processes are used to manage, monitor, and support Pomona College's regulatory, legal, risk, environmental, and operational requirements. These requirements are understood and utilized to inform senior leadership of cybersecurity risk.

INFORMATION SECURITY POLICIES

- Pomona College develops, documents, maintains, and appropriately disseminates information security policies. Policies are approved by senior leadership to provide guidance and address the security controls in place that protect Pomona College's system, assets, and information.
- Pomona College regularly reviews and updates its information security policies, generally on an annual basis.

GOVERNANCE ROLES AND RESPONSIBILITIES

- Pomona College assigns information security roles, responsibilities and coordinates with internal roles and external partners responsible for the different aspects of information security.
- Pomona College's primary information security role will be the Security Official. The Security Official is responsible for implementing and managing all aspects of the information security program at Pomona College. The Security Official is also responsible for bringing risk management recommendations to the Pomona College executive staff.
    - The Deputy Chief Information Officer for Enterprise Services of Pomona College is designated as the Security Official.
- Pomona College's executive staff is responsible for approval of information security policies, risk tolerance, risk treatment, and risk management decisions.

LEGAL AND REGULATORY REQUIREMENTS

- Pomona College's legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood, managed, and communicated.

  Pomona College's legal, regulatory, and other requirements related to cybersecurity include, but are not limited to:
    - Payment Card Industry Data Security Standard (PCI DSS)
    - Family Education Rights and Privacy Act (FERPA)
    - Gramm-Leach-Bliley Act (GLBA[1])
    - Federal Trade Commission (FTC) Act Section 5
    - California security breach notification statutes. (*See* Civ. Code Secs. 1798.29(a), 1798.82(a).)

GOVERNANCE AND RISK MANAGEMENT

- Pomona College governance and risk management processes support a risk management strategy that addresses cybersecurity risks to Pomona College operations, the system, assets, faculty, staff, and students.
- Pomona College risk management strategies are employed consistently across the entire institution.
- The risk management strategies employed by Pomona College are periodically reviewed and updated to address changes to Pomona College.

[1] Pomona College controls related to GLBA compliance are mapped to NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations), as well as the NIST SP-800-53 moderate impact controls.