SYSTEMS RISK MANAGEMENT POLICY

Policy:	Risk 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.RM
NIST SP 800-53 Security Controls	PM-8, PM-9, PM-11, SA-14
NIST SP 800-171 Protecting Controlled Unclassified Information	3.11.3
Center for Internet Security Critical Security Control	CSC 4
Payment Card Industry Data Security Standard (PCI DSS) v3.2	12.2
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

Pomona College maintains a comprehensive strategy to manage risks to its operations, assets, faculty, staff, students, and other organizations associated with the operations and use of Pomona College's system. Pomona College's priorities, constraints, risk tolerances, and assumptions are established and used to support risk management decisions. Pomona College's risk management strategy is consistently applied across the entire institution. The risk management strategy is periodically reviewed and updated, or as required, to address changes to Pomona College.

COMMITMENT TO RISK MANAGEMENT

- To successfully execute its organizational missions, educational, and business functions, Pomona College's executive staff is committed to making risk management a fundamental requirement. This top-level commitment ensures that sufficient resources are available to develop and implement effective, organization-wide risk management practices. The following key elements are necessary for Pomona College to effectively manage information security risks:
  - Assignment of risk management responsibilities to the executive staff.
  - Ongoing recognition and understanding by the executive staff of the information security risks to Pomona College operations, assets, faculty, staff, students, and other organizations associated with the operations and use of Pomona College's system.
  - Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities.
  - Accountability by the executive staff for their risk management decisions and for the implementation of effective, organization-wide risk management.
- Pomona College's risk management processes are established, managed, and agreed to by executive staff.

RISK MANAGEMENT STRATEGY

- The steps in the risk management process are not inherently sequential in nature, but nonetheless include the following steps:
  - Risk Framing
    - Risk framing is the set of assumptions, constraints, risk tolerance, and priorities/trade-offs that shape Pomona College's approach for managing risk. Inputs to the risk framing step include, but are not limited to, laws, policies, regulations, and contractual relationships which impose constraints on potential risk decisions by Pomona College.
  - Assessing Risk
    - Risk assessment identifies, prioritizes, and estimates risk to Pomona College operations, assets, faculty, staff, students, and other organizations associated with the operations and use of Pomona College's system. Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact. For more specifics, please see the **Risk Assessment Policy**.
  - Responding to Risk
    - Risk response identifies, evaluates, decides upon, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to operations, assets, faculty, staff, students, and other organizations associated with the operations and use of Pomona College's system. Decisions on the most appropriate course of action include some form of prioritization, often based on associated cost and/or effort. Some risks may be of greater concern than other risks. In such cases, more resources may need to be directed at addressing higher-priority risks than at other lower-priority risks. This does not necessarily mean that lower-priority risks should not be addressed, rather that fewer resources are directed at lower-priority risks, or that lower-priority risks are addressed later than higher-priority risks.
  - Monitoring Risk
    - Risk monitoring provides Pomona College with the means to:
      - Verify compliance
      - Determine the ongoing effectiveness of risk response measures
      - Identify risk-impacting changes to the Pomona College system

- Analyzing monitoring results gives Pomona College the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

RISK TOLERANCE

- Risk tolerance is the level of risk, or degree of uncertainty, that is acceptable to Pomona College.
- Risk tolerance affects all components of the risk management process, and directly impacts the risk management decisions made by the executive staff.
- Pomona College evaluates risks and applies risk management strategies consistently across the entire institution with respect to Pomona College's defined risk tolerance.