Pomona College

SYSTEMS RISK ASSESSMENT POLICY

Policy:	Risk Assessment
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.RA
NIST SP 800-53 Security Controls	PM-9, PM-11, PM-12, PM-15, PM-16, RA-2, RA-3, RA-5, CA-2, CA-7, CA-8, SI-2, SI-4, SI-5, SA-5, SA-11, SA-14
NIST SP 800-171 Protecting Controlled Unclassified Information	3.11, 3.12
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

Risk assessments take into account threats, vulnerabilities, likelihood, and impact to Pomona College assets, individuals, and other organizations based upon the use of the Pomona College system. Pomona College periodically conducts assessments of risk, which include the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification and/or destruction of the Pomona College system, system components, and the information processed, stored or transmitted by the system. Risk assessment results are documented and reviewed by the Pomona College Security Official or designee. The risk assessment results are then disseminated to appropriate faculty and staff including, but not limited to, the Pomona College executive staff. Risk assessments are conducted annually by Pomona College or whenever there are significant changes to Pomona College, its system, or other conditions that may impact the security of Pomona College.

ASSET VULNERABILITIES

- Pomona College's physical and software assets are assessed and have their vulnerabilities identified and documented periodically.
- Pomona College also employs vulnerability scans. These scans are conducted periodically and identify vulnerabilities in the system and hosted applications.

THREAT AND VULNERABILITY INFORMATION

- Pomona College obtains threat and vulnerability information from information sharing forums and sources. This information is incorporated into the Pomona College asset vulnerabilities documentation.
- Sources for vulnerability and threat information include, but are not limited to:
  - US-CERT Bulletins: https://www.us-cert.gov/ncas/bulletins
  - InfraGard: https://www.infragard.org
  - The Federal Trade Commission: https://www.ftc.gov
  - Research Education Networking Information Sharing & Analysis Center: https://www.ren-isac.net

THREAT IDENTIFICATION

- Threats, both internal and external, to Pomona College operations (including, but not limited to, its mission, functions, image, or reputation), assets, information, and individuals are identified and documented. The threat documentation will include:
  - The type of threats
    - Adversarial
    - Accidental
    - Structural
    - Environmental
  - A description of the threats
  - Characteristics of the threats

THREAT IMPACT AND LIKELIHOOD

- Pomona College's identified threats are evaluated based upon their potential impact to Pomona College, and the likelihood of each threat occurring.
  - Likelihood is determined by:
    - Assessing the likelihood that a threat will be initiated (for adversarial threats) or will occur (for non-adversarial threats)
    - Assessing the likelihood that a threat once initiated or occurring, will result in an adverse impact to Pomona College operations, assets or individuals

        - Assessing the overall likelihood as a combination of likelihood of initiation/occurrence and likelihood of resulting in adverse impact
    - Impact is determined by:
        - The characteristics of a threat that could initiate an event
        - Identified vulnerabilities
        - The ability of safeguards or countermeasures implemented to impede such an event

RISK DETERMINATION

- Pomona College will determine risks based upon identified threats and vulnerabilities, and their impact and likelihood of occurrence to Pomona College.
- Risk is the possibility that a threat will exploit a vulnerability to cause harm to Pomona College operations (including, but not limited to, its mission, functions, image, or reputation), assets, information, and individuals, and is commonly calculated as the product of a threat's impact and its likelihood.

RISK RESPONSE

- Based upon derived risk determinations of threats, Pomona College crafts risk responses. There are four possible responses to risk:
    - Risk reduction or mitigation
        - Risk mitigation is the implementation of safeguards and countermeasures to reduce or eliminate vulnerabilities or block threats.
    - Risk transfer
        - Risk transfer is the placement of the cost of loss a risk represents onto another entity. This is accomplished by purchasing insurance and/or outsourcing.
    - Risk acceptance
        - Acceptance of risk is the valuation by Pomona College that the cost/benefit analysis of a possible safeguard and the determination that the cost of the countermeasure greatly outweighs the possible cost of loss due to a risk. This also means that Pomona College has agreed to accept the consequences and the loss if a risk is realized.
    - Risk rejection
        - Pomona College does not reject risks. Denying that risks exist and hoping that they will never be realized is not an acceptable due-care response to risk