SECURITY OPERATIONS POLICY

Policy:	Security Operations
Policy Owner:	CIO
Change Management	
Original Implementation Date:	8/30/2017
Effective Date:	8/30/2017
Revision Date:	
Approved By:	
Crosswalk	
NIST Cyber Security Framework (CSF)	PR.IP
NIST SP 800-53 Security Controls	AC-21, CM-2, CM-3, CM-4, CM-5, CM-6, CM-9, CP-2, CP-4, CP-6, CP-9, IR-3, IR-8, MP-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, PL-2, PL-8, PM-6, PM-14, RA-3, RA-5, CA-2, CA-7, SI-2, SI-4, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15
NIST SP 800-171 Protecting Controlled Unclassified Information	3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6, 3.6.3, 3.8.1, 3.8.2, 3.8.3, 3.8.9, 3.9.1, 3.9.2, 3.11.1, 3.11.2, 3.11.3, 3.12.1, 3.12.2, 3.12.3, 3.13.1, 3.13.2, 3.14.1, 3.14.2, 3.14.3, 3.14.6, 3.14.7
Center for Internet Security Critical Security Control	3, 4, 7, 10, 11, 19
Payment Card Industry Data Security Standard (PCI DSS) v3.2	1.1, 1.2, 2.2, 2.3, 4.3, 6.1, 6.2, 9.5, 9.6, 9.7, 11.2, 11.5, 12.10
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance to develop and implement the appropriate protective safeguards to ensure the confidentiality, integrity, and availability of Pomona College assets and information.

POLICY

Security operations safeguard Pomona College information assets that reside within the Pomona College information system. These practices help identify threats and vulnerabilities and implement controls to reduce the overall risk to Pomona College assets. Pomona College exercises due care and due diligence by taking reasonable measures to protect its assets on an ongoing and continual basis.

BASELINE CONFIGURATION

- Pomona College develops, documents, and maintains current baseline configurations for its information system and related components.
- Baseline configurations information includes, but is not limited to:
  - Standard software packages for all Pomona College-controlled workstations, laptops, servers, network components, and mobile devices
  - Current version numbers
  - Patch information on operating systems and applications
  - Configuration settings/parameters
  - Network topology
  - The logical placement of components within the system architecture
- Pomona College reviews and updates baseline configuration of the information system:
  - Annually
  - When required due to a major system or business change
  - As an integral part of information system component installations and upgrades
- Pomona College retains previous configuration information to support rollback.
  - Master images are stored on securely configured servers, validated with integrity checking tools to ensure that only authorized changes to the images is possible.
- Pomona College:
  - Requires Faculty and Staff to notify Pomona College ITS when traveling to locations that Pomona College deems to be of significant risk[1]
  - Issues specially configured system components to individuals traveling to locations that Pomona College deems to be of significant risk[1]
  - Applies appropriate safeguards to the specially configured devices upon the return of the individual
  - Protects information residing on mobile devices as part of this control
- Pomona College analyzes changes to its information system to determine potential security impacts prior to change implementation.
- Pomona College defines, documents, approves and enforces physical and logical access restrictions associated with changes to the Pomona College information system.
  - Only qualified and authorized individuals are permitted access to the information system for the purposes of initiating changes, including upgrades and modifications.
- Pomona College:
  - Establishes and documents configuration settings for information technology products employed within the Pomona College information system using defined security configuration checklists that reflect the most restrictive mode consistent with Pomona College's operational requirements
  - Implements the configuration settings
  - Identifies, documents, and approves any deviations from established configuration settings for Pomona College information system components based on requirements defined by Pomona College
  - Monitors and controls changes to the configuration settings in accordance with Pomona College policies and procedures
- Pomona College:
  - Identifies software programs authorized to execute on the Pomona College information system
  - Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the Pomona College system

1 Areas of significant risk are defined as those identified by the US Department of State, Bureau of Consular Affairs: https://travel.state.gov/content/passports/en/alertswarnings.html

- Reviews and updates the list of authorized programs periodically
- Requests to have software added to the authorized to execute designation are to be made directly to the Security Official, or designee.

- Pomona College develops, documents, implements, reviews, and revises a configuration management plan for the Pomona College information system that:
  - Addresses roles, responsibilities, and configuration management processes and procedures
  - Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items
  - Defines the configuration items for the Pomona College information system and places the configuration items under configuration
  - Protects the configuration management plan from unauthorized disclosure and modification
- For internal development and integrations for the Pomona College information system, Pomona College requires:
  - Configuration management during system, component, or service design, development, implementation, and operations
  - Documentation, management, and control of the integrity changes to items under configuration management
  - Implementation of only Pomona College-approved changes to the system, component or service
  - Documentation of approved changes to the system, component, or service and the potential security impacts of such changes
  - Tracking of security flaws and flaw resolution within the system, component, or service and report findings to the Security Official, or designee

SYSTEM DEVELOPMENT LIFE CYCLE

- Pomona College:
  - Manages the Pomona College information system using a waterfall and agile methodologies that incorporate information security considerations
  - Defines and documents the information security roles and responsibilities throughout the system development life cycle
  - Identifies individuals having information security roles and responsibilities
  - Integrates the Pomona College information security risk management process into system development life cycle activities
- Pomona College includes the following requirements, descriptions, and criteria in the acquisition contract for the Pomona College information system, system components, or Pomona College information system service in accordance with applicable state and federal laws, regulations, standards, and policies:
  - Security functional requirements
  - Security strength requirements
  - Security assurance requirements
  - Security-related documentation requirements
  - Requirements for protecting security-related documentation
  - Description of the information system development environment and the environment in which the system is intended to operate
  - Acceptance criteria
- Pomona College requires the developer of the Pomona College information system, system component, or information system service to provide a description of the functional properties of the security controls employed.

- For internal development efforts, Pomona College requires the developer of the Pomona College information system, system component, or information system service to provide design and implementation information for the security controls to be employed. This information may include, but is not restricted to, the following:
  - Security-relevant external system interfaces
  - High-level design
  - Low-level design
  - Source code
  - Hardware schematics
- Pomona College requires the developer of the Pomona College information 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.
- Pomona College applies information system security engineering principles in the specification, design, development, implementation, and modification of the Pomona College information system.
- Pomona College requires the developer of the Pomona College information system, system component, or information system service to:
  - Create and implement a security assessment plan
  - Perform appropriate unit, integration, system, or regression testing
  - Produce evidence of the execution of the security assessment plan and the results of the security testing
  - Implement a verifiable flaw remediation process
  - Correct flaws identified during security testing
- Pomona College protects against supply chain threats to the Pomona College information system, system components, and information system service by employing appropriate safeguards as part of a comprehensive, defense-in-breadth information security strategy.
  - Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement).
  - Protection of Pomona College information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk.
  - This control also applies to information system services. Security safeguards include, for example:
    - Security controls for development systems, development facilities, and external connections to development systems
    - Vetting development personnel
    - Use of tamper-evident packaging during shipping/warehousing.
- Pomona College requires the developer of the Pomona College information system, system components, or information system service to follow a documented development process that:
  - Explicitly addresses security requirements
  - Identifies the standards and tools used in the development process
  - Documents the specific tool options and tools used in the development process
  - Documents the specific tool options and tool configurations used in the development process
  - Reviews the development process, standards, tools, and tool options/configurations at least annually to determine whether the process, standards, tools and tool options/configurations selected and employed can satisfy Pomona College's security requirements

- Pomona College requires the developer of the Pomona College information system, system components, or information system service to produce a design specification and security architecture that:
  - Is consistent with support of Pomona College's information security architecture which is established within and is an integrated part of Pomona College's enterprise architecture
  - Accurately and completely describes the required security functionality, and the allocation of the security controls among physical and logical components
  - Expresses how individual security functions, mechanisms, and services work together to prove required security capabilities and a unified approach to protection
- Pomona College:
  - Develops an information security architecture for the Pomona College information 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 and dependencies on external services
  - Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture
  - Ensures that planning information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurement/acquisitions

3RD PARTY HOSTED SYSTEMS

- Pomona College uses the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to:
  - Reduce the likelihood of unauthorized modifications at each stage in the supply chain
  - Protect information systems and information system components, prior to taking delivery of such systems/components

CONFIGURATION CHANGE MANAGEMENT

- Pomona College:
  - Determines the types of changes to the information system that are configuration-controlled
  - Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses
  - Documents configuration change decisions associated with the Pomona College information system
  - Implements approved configuration-controlled changes to the Pomona College information system
  - Retains records for configuration-controlled changes to the Pomona College information system for 1-year
  - Audits and reviews activities associated with configuration-controlled changes to the Pomona College information system
  - Coordinates and provides oversight for configuration change control activities through a committee that convenes monthly

- Pomona College tests, validates, and documents changes to its information system before implementing the changes on the operational system
  - Testing should be done so that it does not interfere with the information system operations
  - Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted
  - In the event that the information system must be taken off-line for testing, Pomona College will schedule tests during planned system outages whenever possible

DATA BACKUPS

- Pomona College:
  - Regularly conducts backups of user-level information, system-level information, and system documentation including security-related documentation contained in the Pomona College system
  - Protects the confidentiality, integrity, and availability of backup information at storage locations.
- Pomona College tests backup information annually to verify medial reliability and information integrity
- Pomona College:
  - Has established an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information
  - Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site
- Pomona College has identified an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats
- Pomona College has configured the alternate storage site to facilitate recovery operations in accordance with the recovery time and recovery point objective
- Pomona College identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions

DATA RETENTION

- Pomona College handles and retains information within its information system and information outputs from the system in accordance with applicable laws, regulations, policies, standards, and operational requirements
  - **Employees:** When a faculty or staff employee leaves the College, their former account is deactivated per the Pomona College Identity Management, Authentication, and Access Control Policy. All associated data (such as files and/or e-mail associated with that former employee's account) will be retained for four (4) weeks after deactivation and then automatically deleted. The former employee's supervisor, the appropriate Vice President, or Human Resources Management may request an extension to the retention period in writing prior to the end of the four-week period after the employee has left the College.
  - **Students:** Accounts deactivated per the Identity Management, Authentication, and Access Control Policy will be retained for four (4) weeks after deactivation before the account and all associated data such as files and/or e-mail are deleted. Students transitioning to alumni status may retain access to some IT-provided services as provided by the College.
  - **Sponsored Accounts:** When a sponsored account (as defined in the Access Control Policy) is no longer required or the account has reached its expiration time, the account and all associated data (such as files and/or e-mail associated with that former employee's account) will be retained

for four (4) weeks after deactivation and then automatically deleted. Furthermore, the sponsor, the appropriate Vice President or Human Resources may request an extension to the retention period in writing prior to the end of the four-week period after the sponsored account is deactivated.

- **Legal Holds:** From time-to-time, Pomona College may issue subject-matter specific memoranda ("Legal Holds") detailing additional and/or different retention requirements due to pending or threatened litigation, pending or threatened audits, or similar events. Such Legal Holds must be strictly followed, and their provisions supersede any contrary provisions of this Policy
- **Data Retention**: Data maintained on College administrative or learning management systems, such as the Human Resources Information System (HRIS), Finance, Student Information System (SIS), Document Management System, and others may be permanently retained at the discretion of a department or division for such department or division's area of accountability
  - In the event of the death of a Pomona College Student, Faculty, or Staff member Pomona College will retain the individual's data for six (6) months, after which the data will be sanitized in accordance the Data Destruction standard below
  - Human Resources information will be maintained in accordance with legal and Human Resource departmental retention requirements/policies
  - HR information may not be destroyed without prior authorization from the Head of Human Resources.

PHYSICAL OPERATING ENVIRONMENT

- Pomona College:
  - Provides the capability of shutting off power to the Pomona College information system or individual system components in emergency situations
  - Places emergency shutoff switches or devices in locations known to key personnel
  - Protects emergency shutoff capability from unauthorized deactivation
- Pomona College provides a short-term uninterruptible power supply to facilitate the transition of the Pomona College information system to long-term alternate power in the event of a primary power source loss.
- Pomona College provides long-term alternate power supply for the Pomona College information system that is capable of maintaining minimally required operationally capability in the event of an extended loss of the primary power source
- Pomona College employs and maintains automatic emergency lighting for the Pomona College information system that activates in the event of a power outage or disruption.
- Pomona College employs and maintains fire suppression and detection systems that are supported by an independent energy source
- Pomona College employs an automatic fire suppression capability for the Pomona College information system when the facility is not staffed on a continuous basis.
- Pomona College:
  - Maintains the temperature and humidity at acceptable levels within the facility where the Pomona College information system resides
  - Monitors the temperature and humidity levels
    - The temperature and humidity monitoring provides an alarm notifying key personnel of any changes that are potentially harmful to Pomona College personnel or equipment
- The Pomona College information system is protected from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel

- Pomona College positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access

DATA DESTRUCTION

- Pomona College sanitizes information system media prior to disposal, release outside of Pomona College control, or release for reuse.
  - This applies to all information system media, both digital and non-digital, and whether or not the media is considered removable.
  - Examples include, but are not limited to, media found in:
    - Scanners
    - Copiers
    - Printers
    - Laptop computers
    - Desktop computers
    - Network components
    - Mobile devices
  - Sanitization processes for media that will be reused within Pomona College will be chosen based on the sensitivity of the data residing on the media and corresponding risk related to the media's new use
  - Sanitization processes for media leaving the control of Pomona College must remove all information from the media so that the information cannot be retrieved or reconstructed`.
- Pomona College reviews, approves, tracks, documents and verifies media sanitization and disposal actions. Tracking and documentation actions may include, but are not limited to:
  - Listing personnel who reviewed and approved sanitation and disposal actions
  - Types of media sanitized, destroyed, or disposed of
  - Specific files stored on the media
  - Sanitization methods employed
  - Data and time of sanitization and/or destruction actions
  - Personnel who performed the sanitization and/or destruction
  - Verification actions taken
  - Personnel who performed the verification
  - Disposal action taken

CONTINUIOUS IMPROVEMENT

- Pomona College employs a process of continual improvement to its information security program. This process includes the following steps:
  - Prioritize and Scope
    - With the Pomona College mission objectives in mind, Pomona College makes strategic decisions regarding information security implementations and improvements, and determines the scope of these improvements with respect to the information system and Pomona College assets.
    - Implementation tiers may be used to express varying risk tolerances.
  - Orient
    - Once the scope for improvement has been established for the information security program, Pomona College then identifies related systems, assets, regulatory requirements, and overall

risk approach. Pomona College then consults sources to identify threats and vulnerabilities applicable to those assets and systems.

- Profile
  - Pomona College next develops and/or updates a current profile indicating which aspects of applicable security framework outcomes are currently being achieved. If an outcome is partially achieved, then noting this fact will help support subsequent steps.
- Risk Assessment
  - Pomona College conducts a risk assessment in accordance with its risk assessment policy. This risk assessment may be guided by the Pomona College risk management strategy and/or previous risk assessments.
- Create Target Profile
  - Pomona College creates a target profile that focuses on the risk assessment findings, and the current profile. The target profile describes Pomona College's desired information security outcomes.
- Determine, Analyze, and Prioritize Gaps
  - Pomona College compares the current profile and the target profile to determine any gaps.
  - Pomona College then creates a prioritized action plan to address those gaps drawing upon various input sources such as mission drivers, a cost/benefit analysis, and risk understanding to achieve the outcomes of the target profile.
  - Pomona College then determines the necessary resources to address the gaps.
- Implement Action Plan
  - Pomona College determines which actions to take regarding the gaps, if any, that were identified in the previous step.
  - Pomona College then monitors its current information security program against the target profile.

- Pomona College repeats the improvement process as needed to continuously assess and improve its information security program.

EFFECTIVENESS SHARING

- Pomona College shares the effectiveness of protection technologies with appropriate parties.
  - Appropriate parties may be internal or external depending upon the nature of the protection technologies and that of any information to be shared.

RESPONSE AND RECOVERY PLAN MANAGEMENT

- Pomona College employs the following response plans and recovery plans:
  - Response Plans:
    - Incident Response Plan
    - Business Continuity Plan
  - Recovery Plans:
    - Incident Recovery Plan
    - Disaster Recovery Plan
- The Incident Response Plan establishes procedures to address events that have the potential to negatively impact the confidentiality, integrity, and/or availability of the Pomona College information system and/or its information. These procedures enable security personnel to identify and mitigate incidents such as unauthorized access to Pomona College confidential information, or to respond to unauthorized changes to system hardware, software or data.

- The Business Continuity Plan (BCP) focuses on sustaining Pomona College's mission and business processes during and after a disruption.
- The Incident Recovery Plan includes procedures that enable security personnel to recover from incidents identified and mitigated by the Incident Response Plan.
- The Disaster Recovery Plan (DRP) applies to major, usually physical, disruptions to service that deny access to Pomona College's primary facility infrastructure for an extended period of time. The DRP is an information system-focused plan intended to restore operability of the Pomona College information system at an alternate site after an emergency. The DRP supports the BCP by recovering supporting systems for Pomona College mission processes. The DRP only addresses information system disruptions that require relocation of operations.

RESPONSE AND RECOVERY PLAN TESTING

- Pomona College tests the Business Continuity, Disaster Recovery, and Incident Response & Recovery Plan annually. These test results are reviewed and any necessary corrective actions are taken. Types of tests employed by Pomona College may include:
  - Walk-through exercises
  - Tabletop exercises
  - Checklists
  - Parallel simulations
  - Full interrupt simulations.