PROTECTIVE TECHNOLOGY POLICY

Policy:	Protective Technology
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.PT
NIST SP 800-53 Security Controls	AC-3, AC-4, AC-17, AC-18, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, AU-15, AU-16, CM-7, CP-7 CP-8, CP-11, CP-13, MP-2, MP-4, MP-5, MP-7, PL-8, SC-2, SC-6, SC-7, SA-14
NIST SP 800-171 Protecting Controlled Unclassified Information	3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.7, 3.3.8, 3.3.9
Center for Internet Security Critical Security Control	5, 7, 14
Payment Card Industry Data Security Standard (PCI DSS) v3.2	10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.9
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

Pomona College employs and manages technical security solutions to ensure the security and resilience of the Pomona College system and its components, as well as Pomona College assets and personnel.

AUDIT LOGS

- Pomona College:
  - Has determined which events the Pomona College system is capable of logging
  - Coordinates the security audit function with other Pomona College departments and/or teams requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
  - Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents

- Determines which events of those that can be logged are to be logged within the Pomona College system

- Pomona College reviews and updates the existing set of logged events quarterly to ensure that the current set is necessary and sufficient
- The Pomona College system generates audit records containing information that establishes what type of event occurred, when the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
  - Pomona College system logs include, but are not limited to, the following types of information regarding events:
    - Date
    - Timestamp
    - Source addresses
    - Destination addresses
  - Pomona College system components record logs in a standardized format. In the event that a system component is unable to generate logs in a standardized format, log normalization tools are deployed to convert logs into such format.
  - The Pomona College system generates log records containing the full text recording of privilege commands
- Pomona College allocates appropriate log file storage capacity to reduce the likelihood of such capacity being exceeded and resulting in the loss or reduction of auditing capability
- In the event of an audit processing failure, the Pomona College system:
  - Alerts Security Official, or designee in the event of an audit processing failure
  - Takes the following actions:
    - Stop generating audit records
    - Determine root cause of audit processing failure
    - Return to normal operations
- Pomona College:
  - Reviews and analyzes the Pomona College system logs biweekly for indications of inappropriate, unusual, or anomalous activity
  - Inappropriate, unusual, or anomalous activities are documented and reported to the Security official, or designee
- Pomona College employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
- Pomona College analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
- The Pomona College system provides an audit reduction and report generation capability that:
  - Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents
  - Does not alter the original content or time ordering of audit records
- The Pomona College system provides the capability to process audit records of events of interest based on identities of individuals, event types, event locations, event times, event dates, system resources involved, IP Addresses involved, and information object accessed.
- The Pomona College system:
  - Uses internal system clocks to generate time stamps for audit records
  - Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC)
  - Compares the internal system clocks every 24-hours with at least two synchronized external time sources

- Synchronizes the internal system clocks to the authoritative time sources when the time difference is greater than one second

- The Pomona College system protects audit information and audit tools from unauthorized access, modification, and deletion.
- Pomona College authorizes access to management of audit functionality only to individuals with administrative privileges specific to the systems generating the audits.
- The Pomona College system protects against an individual, or process acting on behalf of an individual, falsely denying having performed actions that are captured in the audited system events.
- Pomona College retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational retention requirements.
  - Pomona College retains audit records for 30 days in easily accessible storage media.
  - Older logs are archived on less expensive storage media and are retained as is required by incidents or investigations.
- The Pomona College system:
  - Provides audit record generation capability for auditable events
  - Allows for authorized personnel to select which auditable events are to be audited by specific system component
  - Generates audit records for the events that events determined to be audited
- Pomona College monitors its confidential information for evidence of unauthorized disclosure.

REMOVABLE MEDIA PROTECTION

- Pomona College:
  - Protects and controls removable media containing confidential information during transport outside of Pomona College controlled areas using strong encryption technologies
  - Maintains accountability for Pomona College system media during transport outside of controlled areas
  - Documents activities associated with the transport of Pomona College system media
  - Restricts the activities associated with the transport of system media to authorized personnel
- The Pomona College system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of Pomona College controlled areas
- Pomona College controls the use of removable media on Pomona College system components
- Pomona College prohibits the use of portable storage devices in the Pomona College system when such devices have no identifiable owner

LEAST FUNCTIONALITY

- Pomona College:
  - Configures the Pomona College system to provide only essential capabilities
  - Prohibits, restricts, or disables unnecessary, ports, functions, protocols, and/or services.
  - Reviews the system annually to identify unnecessary and/or non-secure functions, ports, protocols, and services

- The Pomona College system prevents program execution in accordance with Pomona College policies including, but not limited to, the Pomona College Acceptable Use policy
- The Pomona College system separates user functionality (including user interface services) from system management functionality
- Pomona College:
  - Identifies software programs authorized to execute on the Pomona College system
  - Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the Pomona College system
  - 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 Deputy Chief Information Officer (Client, Media and Instructional Services), or designee

COMMUNICATIONS AND NETWORK PROTECTION

- The Pomona College system enforces approved authorizations for controlling the flow of information within the system and between any interconnected systems.
- Pomona College:
  - Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for wireless access.
  - Authorizes wireless access to the Pomona College system prior to allowing such connections.
- The Pomona College system protects wireless access to the system using authentication of users and encryption.
- Pomona College:
  - Ensures that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Internal wireless access is denied to wireless devices that do not possess an authorized configuration and security profile.
  - Configures network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices are reconciled against a list of authorized wireless access points. Unauthorized access points are deactivated.
- Pomona College:
  - Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks.
  - Allows connections to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the Pomona College security architecture.
- Pomona College limits the number of external network connections to the Pomona College system in order to facilitate a more comprehensive monitoring of inbound and outbound network traffic.
- Pomona College:
  - Implements a managed interface for each external telecommunication
  - Establishes a traffic flow policy for each managed interface
  - Protects the confidentiality and integrity of the information being transmitted across each interface
  - Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need
  - Reviews exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need

- The Pomona College system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception.
- The Pomona College system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.
- The Pomona College system fails securely in the event of an operational failure of a boundary protection device.