CONTINUOUS VIGILANCE POLICY

Policy:	Continuous Vigilance
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)	DE.CM
NIST SP 800-53 Security Controls	AC-2, AU-6, AU-12, AU-13, CM-3, CM-10, CM-11, PS-7, PE-3, PE-6, PE-20, PL-2, PM-13, PM-14, RA-5, CA-7, CA-8, SC-5, SC-7, SC-18, SC-44, SI-3, SI-4, SA-9
NIST SP 800-171 Protecting Controlled Unclassified Information	3.1.1, 3.1.2, 3.1.12, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.9, 3.4.9, 3.9.2, 3.10.2, 3.10.3, 3.10.4, 3.10.5, 3.11.2, 3.11.3, 3.12.1, 3.12.2, 3.12.3, 3.3.4, 3.12.2, 3.12.3, 3.12.4 3.13.1, 3.13.2, 3.13.5, 3.13.6, 3.13.7, 3.13.13, 3.14.1, 3.14.2, 3.14.3, 3.14.4, 3.14.5, 3.14.6, 3.14.7
Center for Internet Security Critical Security Control	4, 6, 8, 19
Payment Card Industry Data Security Standard (PCI DSS) v3.2	5.1, 5.2, 5.3, 5.4, 6.1, 9.1, 9.2, 9.10, 10.1, 10.2, 10.3, 10.6, 11.2, 11.4, 11.6,
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance to develop and implement the appropriate activities to identify the occurrence of an information security event.

POLICY

The Pomona College system, system components, and assets are monitored at discrete intervals to identify information security events and to verify the effectiveness of protective measures.

Pomona College detection processes and procedures are maintained to provide for the identification of information security events. Detection processes are tested and revised to ensure the timely notification of anomalous events to the appropriate Pomona College responsible parties.

NETWORK VIGILANCE

- Pomona College has developed a continuous vigilance strategy for the Pomona College network that is a part of the Pomona College Continuous Vigilance Program and includes:

- Establishment of network metrics that are monitored
- Ongoing security control assessments in accordance with Pomona College's Continuous Vigilance Program
- Ongoing security status monitoring of defined metrics in accordance with Pomona College's Continuous Vigilance Program
- Correlation and analysis of security-related information gathered by assessments and monitoring
- Response actions to address results of the analyses of security-related information

- Pomona College:
  - Monitors the network to detect:
    - Attacks and indicators of potential attacks in accordance with the Pomona College Continuous Vigilance Program
    - Unauthorized network and remote connections
  - Identifies unauthorized use of the network
  - Deploys monitoring devices strategically within the network to collect essential information
  - Protects information obtained from intrusion-monitoring tools from unauthorized access, modification and deletion
  - Heightens the level of network vigilance activity whenever there is an indication of increased risk to Pomona College operations and assets, individuals, other organizations, or the United States based on law enforcement information, intelligence information, or other credible sources of information
  - Obtains legal opinion with regard to focused network vigilance activities in accordance with applicable state and federal laws
  - Provides network vigilance information to the Security Official, or designee, on a monthly basis
- Pomona College:
  - Determines the types of changes to the network that are configuration-controlled
  - Reviews proposed configuration-controlled changes to the network and either approves or disapproves such changes with explicit consideration for security impact analysis
  - Documents configuration change decisions associated with the network
  - Implements approved configuration-controlled changes to the network
  - Tests, validates, and documents changes to the network before implementation
  - Retains records of configuration-controlled changes to the network
  - Coordinates and provides oversight for configuration change control activities with ITS Leadership on a quarterly basis
- The Pomona College network:
  - Provides audit record generation capability for auditable events
  - Allows authorized users to select which auditable events are to be audited
- The Pomona College network generates audit records for the network events selected.

PHYSICAL ENVIRONMENT VIGILANCE

- Pomona College has developed a continuous vigilance strategy for its physical environment that is part of the Pomona College Continuous Vigilance Program, and includes:
  - Establishment of physical environment metrics to be monitored
  - Establishment of frequency of physical environment vigilance and quarterly assessments for supporting such monitoring
  - Ongoing security control assessments in accordance with Pomona College's Continuous Vigilance Program

- Ongoing security status monitoring of defined metrics in accordance with Pomona College's Continuous Vigilance Program
- Correlation and analysis of security-related information gathered by assessments and monitoring
- Response actions to address results of the analyses of security-related information
- Reporting the security status of Pomona College and the Pomona College's physical environment to the Security Official, or designee, on a monthly basis

- Pomona College employs independent assessors to evaluate the Pomona College's physical environment security controls.
- Pomona College enforces physical access controls[1].
- Pomona College:
  - Monitors physical access to the facility where the Pomona College system resides to detect and respond to physical security incidents
  - Monitors physical intrusion alarms and surveillance equipment
  - Employs video surveillance of sensitive and high risk areas and normally retains video recordings for up to 30 days
  - Reviews physical access logs quarterly and upon occurrence of potential indications of an event
  - Coordinates results of reviews and investigations with the Pomona College Incident Response Team
- Pomona College:
  - Employs asset location technologies to track and monitor the location and movement of Pomona College system components and assets
  - Ensures that asset location technologies are employed in accordance with applicable state and federal laws and regulations

PERSONNEL VIGILANCE

- Pomona College has developed a continuous vigilance strategy for its personnel that is part of the Pomona College Continuous Vigilance Program, and includes:
  - Establishment of user metrics to be monitored
  - Establishment of frequency of personnel vigilance and quarterly assessments for supporting such monitoring
  - Ongoing security control assessments in accordance with Pomona College's Continuous Vigilance Program
  - Ongoing security status monitoring of defined metrics in accordance with Pomona College's Continuous Vigilance Program
  - Correlation and analysis of security-related information gathered by assessments and monitoring
  - Response actions to address results of the analyses of security-related information
  - Reporting the security status of Pomona College and Pomona College's personnel to the Security Official, or designee, on a monthly basis
- Pomona College monitors the Pomona College system for evidence of unauthorized disclosures of Pomona College organizational information.
- Pomona College employs account management controls to assist in personnel vigilance[2].

MALWARE

[1] See Identity Management, Authentication, and Access Control Policy
[2] See Identity Management, Authentication, and Access Control Policy

- Pomona College:
  - Employs malicious code protection mechanisms at information entry and exit points to detect and eradicate malicious code
    - Malicious code protection mechanisms include automated tools that continuously monitor workstations, servers and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based Intrusion Protection System (IPS) functionality
  - Updates malicious code protection mechanism whenever new releases are available in accordance with Pomona College configuration management policy and procedures
    - After updates are applied, automated systems verify that each system component has received its signature update
  - Configures malicious code protection mechanisms to:
    - Perform periodic scans of the Pomona College system and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed
    - Block and quarantine malicious code as well as send an alert to administrators in response to malicious code detection
    - Address the receipt of false positives during malicious code detection, eradication and the resulting potential impact on the availability of the Pomona College system
  - Employs network-based tools to identify executables in all network traffic and uses techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint
  - Has enabled domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains
  - Centrally manages malicious code protection mechanisms
    - All malware detection events are sent to centrally managed anti-malware administration tools and event log servers
- The Pomona College system automatically updates malicious code protection mechanisms.
- Pomona College:
  - Limits the use of external devices to those with an approved, documented business need
  - Monitors for use and attempted use of external devices
  - Configures laptops, workstations, and servers so that they will not auto-run content from removable media, USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares
  - Configures systems so that they automatically conduct an anti-malware scan of removable media when inserted into system components
- Pomona College:
  - Has enabled anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and virtualization/containerization
    - Enhanced Mitigation Experience Toolkit (EMET) may be deployed to apply the above protections to a broader set of applications and executables

MOBILE CODE

- Pomona College:
  - Defines acceptable and unacceptable mobile code and mobile code technologies
  - Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies
  - Authorizes, monitors, and controls the sue of mobile code within the Pomona College system

THIRD PARTY VIGILANCE

- Pomona College has developed a continuous vigilance strategy for third parties that is part of the Pomona College Continuous Vigilance Program, and includes:
  - Establishment of third-party metrics to be monitored
  - Establishment of frequency of third-party and quarterly assessments for supporting such monitoring
  - Ongoing security control assessments in accordance with Pomona College's Continuous Vigilance Program
  - Ongoing security status monitoring of defined metrics in accordance with Pomona College's Continuous Vigilance Program
  - Correlation and analysis of security-related information gathered by assessments and monitoring
  - Response actions to address results of the analyses of security-related information
  - Reporting the security status of Pomona College and the Pomona College's third parties to the Security Official, or designee, on a monthly basis
- Pomona College:
  - Establishes third-party personnel security requirements that include roles and responsibilities
  - Requires third-party providers to comply with Pomona College personnel security policies and procedures
  - Requires third-party providers to notify the Pomona College Security Official, or designee, of any personnel transfers or terminations of third-party personnel who possess Pomona College credentials and/or badges, or who have privileges to the Pomona College system
- Pomona College:
  - Requires that providers of external system services comply with Pomona College information security requirements and employ reasonable security controls in accordance with state and federal laws and regulations
  - Defines and documents government oversight and user roles and responsibilities with regard to external system services
  - Monitors the security control compliance by external service providers on an ongoing basis
  - Establishes, documents, and maintains trust relationships with external service providers

SYSTEM VIGILANCE

- Pomona College:
  - Monitors the Pomona College system to detect:
    - Attacks and indicators of potential attacks in accordance with the Pomona College Continuous Vigilance Program
    - Unauthorized network and remote connections
  - Identifies unauthorized use of the Pomona College system
  - Deploys monitoring devices strategically within the Pomona College system to collect essential information
  - Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion
  - Heightens the level of Pomona College system vigilance activity whenever there is an indication of increased risk to Pomona College operations and assets, individuals, other organizations, or the United States based on law enforcement information, intelligence information, or other credible sources of information

- May obtain legal opinion with regard to Pomona College system enhanced vigilance activities in accordance with applicable state and federal laws
- Provides system vigilance information to the Security Official, or designee, on a monthly basis

- Pomona College has developed a continuous vigilance strategy for the Pomona College system that is a part of the Pomona College Continuous Vigilance Program and includes:
  - Establishment of system metrics that are monitored
  - Establishment the frequency of system vigilance and the quarterly assessments for supporting such monitoring
  - Ongoing security control assessments in accordance with Pomona College's Continuous Vigilance Program
  - Ongoing security status monitoring of defined metrics in accordance with Pomona College's Continuous Vigilance Program
  - Correlation and analysis of security-related information gathered by assessments and monitoring
  - Response actions to address results of the analyses of security-related information
  - Reporting the security status of Pomona College and the Pomona College system to the Security Official, or designee, on a monthly basis

VULNERABILITY MANAGEMENT

- Pomona College:
  - Contracts with a Payment Card Industry Security Standards Council (PCI SSC) Approved Scanning Vendor (ASV) to conduct quarterly external vulnerability scans of the Pomona College system and appropriate hosted applications
  - Contracts with an ASV to conduct quarterly internal vulnerability scans of the Pomona College system and appropriate hosted applications
  - Conducts its own vulnerability scans weekly of the Pomona College system and hosted applications
  - Retains vulnerability scan reports for at least twelve (12) months
  - Scans for vulnerabilities in the Pomona College system and hosted applications when new vulnerabilities potentially affecting the system or applications are identified and reported
  - Employs vulnerability scanning tools and techniques to facilitate interoperability among tools and automate portions of the vulnerability management process by using standard approaches for:
    - Enumerating platforms, software flaws, and improper configurations
    - Formatting checklists and test procedures
    - Describing vulnerability impact
  - Analyzes vulnerability scan reports and results from security control assessments, risk assessments, and compliance audits
  - Correlates event logs with information from vulnerability scans to fulfill goals:
    - Personnel should verify that the activity of the regular vulnerability scanning tools is itself logged
    - Personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable
  - Remediates legitimate vulnerabilities in accordance with its assessment of risk and the risk management strategy
  - Upon vulnerability remediation, rescans until passing scans are needed

- Shares information obtained from the vulnerability scanning process and security control assessments with the Claremont University Consortium to help eliminate similar vulnerabilities in other systems
- Employs vulnerability scanning tools that include the capability to readily update the system vulnerabilities to be scanned
- Updates the Pomona College system vulnerabilities scanned at least annually, prior to any new scans, and when new vulnerabilities are identified or reported
- Implements privileged access authorization to key system components of the Pomona College system for vulnerability scanning activities
- Subscribes to vulnerability intelligence services so as to stay aware of emerging exposures
- Monitors logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans
- Compares the results of back-to-back scans to verify that the vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting reasonable business risk
- Has established a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets
  - Patches are then applied for the highest risk vulnerabilities first

PENETRATION TESTING

- Pomona College:
  - Performs external penetration testing annually and after any significant changes to the Pomona College system or application upgrade or modification
    - External penetration tests are conducted by either qualified internal resources or a qualified external third-party[3]
  - Performs internal penetration testing annually and after any significant changes to the Pomona College system, application upgrade or modification
    - Internal penetration tests are conducted by either qualified internal resources or a qualified external third-party[4]
  - Mitigates any exploitable vulnerabilities found during penetration testing
  - Performs repeat penetration testing after vulnerability mitigation to verify mitigation
-

DETECTION PROCESSES ROLES AND RESPONSIBILITIES

- Pomona College establishes roles within its workforce that are assigned to monitor and report on the detection processes employed by Pomona College.
- Pomona College:
  - Implements processes for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with detection processes:
    - Are developed and maintained
    - Continue to be executed in a timely manner

[3] Not required to be a QSV or ASV
[4] Not required to be a QSV or ASV

- Reviews testing, training, and monitoring of plans consistency with the Pomona College risk management strategy

DETECTION PROCESS REQUIREMENTS

- Pomona College:
  - Implements processes for the conducting of testing, training, and monitoring activities associated with Pomona College's detection processes
  - Ensures that detection process activities comply with all applicable requirements

CONTINUOUS IMPROVEMENT OF DETECTION PROCESSES

- As part of its plan of action and milestones, Pomona College:
  - Includes reviews, testing, and updating of the Pomona College detection processes
  - Reviews testing, training, and monitoring plans associated with the detection processes for consistency with Pomona College's risk management strategy
- Pomona College periodically tests the event detection processes.
- Pomona College:
  - Regularly reviews the event detection processes
  - Reviews the event detection processes in the event of a significant change affecting event detection
- Pomona College:
  - Updates the event detection processes according after reviews
  - Updates to the event detection processes are consistent with the Pomona College risk management strategy

EVENT DETECTION COMMUNICATION

- Pomona College:
  - Reviews and analyzes event detection records and logs regularly
  - Event detection information is communicated to appropriate parties in a timely manner to the Security Official, or designee