INCIDENT RESPONSE POLICY

Policy:	Incident Response
Policy Owner:	CIO
Change Management	
Original Implementation Date:	3/7/2018
Effective Date:	3/7/2018
Revision Date:	
Approved By:	Executive Staff
Crosswalk	
NIST Cyber Security Framework (CSF)	RS.RP, RS.CO, RS.AN, RS.MI, RS.IM
NIST SP 800-53 Security Controls	AU-6, AU-7, CP-2, CP-3, CP-10, IR-2, IR-3, IR-4, IR-5, IR-6, IR-8, PE-6, PM-15, RA-3, RA-5, CA-2, CA-7, SI-4, SI-5
NIST SP 800-171 Protecting Controlled Unclassified Information	3.6.1, 3.6.2, 3.6.3
Center for Internet Security Critical Security Control	19
Payment Card Industry Data Security Standard (PCI DSS) v3.2	
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance to developing and implementing the appropriate activities to take action regarding a detected information security event.

POLICY

Pomona College has an Incident Response Plan (IRP) that addresses the processes and procedures to be executed and maintained, to ensure timely response to a detected information security event. Analysis of detected information security events is conducted, by Pomona College, to ensure adequate response and to support recovery activities. Upon detection of an information security event, Pomona College will take the necessary actions to prevent the expansion of an event, to mitigate its effects, and eradicate the incident. Upon mitigation of an information security event, Pomona College will incorporate lessons learned into the Incident Response Plan to improve upon it.

RESPONSE PLAN

- Pomona College:
  - Develops an Incident Response Plan (IRP) that:
    - Provides Pomona College with a roadmap for implementing its incident response capabilities

        - Describes the structure and organization of the incident response capabilities
        - Provides a high-level approach for how the incident response capabilities fit into the overall organization
        - Meets the unique requirements of Pomona College, which relate to the College's mission, its size, structure, and functions
        - Defines reportable incidents
        - Provides metrics for measuring the incident response capabilities within Pomona College
        - Defines the resources and management support needed to effectively maintain and mature an incident response capability
        - Is reviewed and approved by the Security Official
    - Distributes the IRP at least annually, and after any significant revisions
    - Reviews the incident response plan annually, and if deemed appropriate from an incident post-mortem risk assessment
    - Updates the IRP to address
        - Organizational changes
        - Changes to the Pomona College system
        - Problems encountered during plan implementation, execution, or testing
    - Communicates IRP changes to appropriate faculty and staff
    - Protects the IRP from unauthorized disclosure and modification
- Pomona College tests its incident response capabilities at least annually to determine the effectiveness of its incident response.
    - Pomona College coordinates incident response testing with organizational elements responsible for related plans (i.e., BCPs and DRPs).
- Pomona College:
    - Implements its incident handling capabilities for security incidents that includes related preparation, detection and analysis, containment, eradication, and recovery
    - Coordinates incident handling activities with contingency planning activities
    - Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly
    - Employs automated mechanisms to support the incident handling process
    - Tracks and documents security incidents handling activities

INCIDENT RESPONSE COMMUNICATIONS

- Incident response activities are coordinated with internal and external stakeholders, and, where appropriate, external support from law enforcement agencies
- Pomona College informs faculty and staff of their roles and responsibilities when a response to an incident is needed
- Pomona College provides incident response training to faculty and staff consistent with assigned roles and responsibilities:
    - Within no more than 30 days of assuming an incident response role or responsibility
    - When required by system changes
    - Annually thereafter
- Pomona College incorporates simulated events into incident response training to facilitate effective response by faculty and staff in crisis situations.
- Pomona College employs automated mechanisms to provide a more thorough and realistic incident response training environment.
- Pomona College:

- Requires faculty and staff to report suspected security incidents to the Security Official, or designee
- Employs automated mechanism to assist in the reporting of security incidents

- Pomona College coordinates and shares information with internal and external stakeholders, and law enforcement in a manner consistent with the IRP.

INCIDENT DETECTION AND ANALYSIS

- The Pomona College system is capable of detecting indicators of a security incident; security incident indicators include, but are not limited to:
  - Network intrusion detection sensor alerts
  - Antivirus software alerts
  - A system administrator sees a filename with unusual characters
  - A host records an auditing configuration change in its log
  - An application logs multiple failed login attempts
  - An email administrator notices a large number of bounced emails
  - A network administrator notices an unusual deviation from typical network traffic flows
- In response to an incident, Pomona College will analyze and validate each incident
  - Pomona College will document each step taken in the analysis and validation of incidents
- Upon confirmation of an incident, Pomona College will perform an initial analysis to determine:
  - The incident's scope
  - Who or what originated the incident
  - How the incident is occurring
- Pomona College's incident documentation shall contain the following information:
  - Current status of the incident
  - Summary of the incident
  - Indicators related to the incident
  - Other incidents related to this incident
  - Actions taken by all incident handlers on this incident
  - Chain of custody, if applicable
  - Impact assessment related to the incident
  - Contact information for other involved parties
  - A list of evidences gathered during the incident investigation
  - Comments from incident handlers
  - Next steps to be taken
- Pomona College safeguards incident data and restricts access to individuals on a need-to-know basis
- Pomona College prioritizes the handling of incident based upon the following factors:
  - Functional impact of the incident
  - Information impact of the incident
  - Recoverability from the incident

CONTAINMENT, ERADICATION, AND RECOVERY

- Pomona College maintains separate containment strategies for each major incident type, with criteria documented to facilitate the decision-making of the appropriate type of containment strategy to be employed
  - Criteria for determining the appropriate containment strategy include:
    - Potential damage to and theft of resources

- Need for evidence preservation
- Service availability
- Time and resources needed to implement the strategy
- Effectiveness of the strategy
- Duration of the solution

- Pomona College gathers security incident evidence to help resolve the incident, as well as for legal proceedings if needed
- All evidence, including compromised systems, are preserved
- Evidence is collected according to procedures that meet all applicable laws and regulations
- Evidence is accounted for at all times, whenever evidence is transferred from person to person, Pomona College documents chain of custody
- Pomona College maintains a detailed log of all evidence that includes:
  - Identifying information
  - Name, title, and phone number of each individual who collected or handled the evidence during the investigation
  - Time and date of each occurrence of evidence handling
  - Locations where evidence was stored
- After an incident has been contained, eradication may be necessary to eliminate components of the incident
- During eradication, Pomona College identifies all affected hosts so that they can be remediated
- For some incidents, eradication is either not necessary or is performed during recovery
- In recovery, Pomona College restores systems to normal operation, confirms that the systems are functioning normally, and, if applicable, remediates vulnerabilities to prevent future-like incidents.
- Recovery actions may include, but are not limited to:
  - Restoring systems from clean backups
  - Rebuilding systems from scratch
  - Replacing compromised files with clean versions
  - Installing patches
  - Changing passwords
  - Tightening network perimeter security

POST-INCIDENT ACTIVITY

- Pomona College holds “lessons learned” meetings after every major security incident, and optionally after lesser incidents if appropriate
- Questions to be answered in “lessons learned” meetings include:
  - Exactly what happened, and at what times?
  - How well did staff and management perform in dealing with the incident?
  - Where documented procedures followed, and were they adequate?
  - What information was needed sooner?
  - Were any steps or actions taken that might have delayed or otherwise inhibited the recovery?
  - What would the staff and management do differently the next time a similar incident occurs?
  - How could information sharing with other organizations have been improved?
  - What corrective actions can prevent future-like incidents?
  - What precursors or indicators should be watched for in the future to detect similar incidents?
  - What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
- Pomona College will create a follow-up report for each incident
- Pomona College will produce objective and subjective data regarding each incident

- This data will be cycled back into the Pomona College risk assessment process to assist in the development and improvement of Pomona College's risk management strategy
- The incident related data includes, but is not limited to:
  - Number of incidents handled
  - Time per incident
  - Objective assessment of each incident
  - Subjective assessment of each incident