SECURITY EVENTS AND ANOMALIES POLICY

<table>
<thead>
<tr>
<th>Policy:</th>
<th>Security Events and Anomalies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Owner:</td>
<td>CIO</td>
</tr>
<tr>
<td>Change Management</td>
<td></td>
</tr>
<tr>
<td>Original Implementation Date:</td>
<td>8/30/2017</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>8/30/2017</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>Approved By:</td>
<td></td>
</tr>
<tr>
<td>Crosswalk</td>
<td></td>
</tr>
<tr>
<td>NIST Cyber Security Framework (CSF)</td>
<td>DE, AE</td>
</tr>
<tr>
<td>NIST SP 800-53 Security Controls</td>
<td>AC-4, AU-6, CM-2, IR-4, IR-5, IR-8, CA-3, RA-3, CA-7, SI-4</td>
</tr>
<tr>
<td>NIST SP 800-171 Protecting Controlled Unclassified Information</td>
<td>3.1.3, 3.1.12, 3.1.13, 3.1.14, 3.1.15, 3.1.18, 3.1.20, 3.1.21, 3.1.22, 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, 3.4.7, 3.6.1, 3.6.2, 3.6.3, 3.13.1, 3.13.12, 3.13.13, 3.13.15, 3.13.16, 3.13.17, 3.13.18, 3.14.7</td>
</tr>
<tr>
<td>Center for Internet Security Critical Security Control</td>
<td>6, 9, 12, 19</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard (PCI DSS) v3.2</td>
<td>1.1, 1.2, 1.3, 1.4, 8.3, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 11.4, 12.10</td>
</tr>
</tbody>
</table>

**PURPOSE**

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

**POLICY**

Pomona College employs controls to detect anomalous activity in a timely manner. Information regarding detected anomalous activity is gathered in order to understand the potential impact to Pomona College.

**NETWORK OPERATIONS BASELINE**

- Pomona College develops, documents, and maintains under configuration control, a baseline configuration of the Pomona College system's network operations.
- Pomona College reviews and updates the network operations baseline configuration:
  - Annually or
  - When required, due to an identified vulnerability, or
  - As an integral part of installations and/or upgrades to the network
The Pomona College system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.

- All outgoing network traffic to the internet must pass through at least one application-layer filtering proxy server
  - The proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a blocklist, and applying a list of allowed sites that can be accessed through the proxy while blocking all other sites.

Pomona College:

- Authorizes connections from the Pomona College system to other systems through the use of Interconnection Security Agreements
- Employs deny-all, permit-by-exception for connections between the Pomona College system and external systems
- Documents for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated
- Reviews and updates the Interconnection Security Agreements annually

SECURITY EVENT DETECTION AND ANALYSIS

Pomona College:

- Configures monitoring systems on Demilitarized Zone (DMZ) networks to record:
  - At minimum, packet header information and if possible full packet header
  - Preferably full packet header and payloads of the traffic destined for or passing through the network border
- Deploys NetFlow collection and analysis
- Deploys monitoring devices:
  - Strategically within the Pomona College system to collect essential information
    - This includes network-based IDS sensors on internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromises of these systems.
    - At ad hoc locations within the Pomona College system to track specific types of transactions of interest to Pomona College
  - Employs automated tools to support near real-time analysis of events
  - Periodically scans for back-channel connections to the internet
- The Pomona College system monitors inbound and outbound network connections for unusual or unauthorized activities or conditions.
  - Network boundary devices, including, but not limited to, firewalls, network-based IPS, and inbound and outbound proxies, are configured to verbose log all traffic arriving at the devices, both allowed and blocked.
  - Network based IPS devices are deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks.
- The Pomona College system alerts the Security Incident Response Team (SIRT) when indications of a compromise or potential compromise occur.

EVENT CORRELATION

Pomona College correlates security event information and incident responses to achieve an organization-wide perspective on incident awareness and response.
EVENT IMPACT

- Events are assessed by Pomona College utilizing the Pomona College risk assessment methodology in order to determine the potential impact of detected security events.
  - The results of security event risk assessments are documented in risk assessment reports.
  - Security event risk assessment reports are reviewed by the Security Official, or designee, and then disseminated to any appropriate personnel across the college.
- Pomona College coordinates incident handling activities with contingency planning activities.

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