TRAINING AND AWARENESS POLICY

Policy:	Training and Awareness
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.AT
NIST SP 800-53 Security Controls	AT-2, AT-3, PS-7, PM-13, SA-9
NIST SP 800-171 Protecting Controlled Unclassified Information	3.2
Center for Internet Security Critical Security Control	CSC 5, 17
Payment Card Industry Data Security Standard (PCI DSS) v3.2	2.1, 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 8.7, 12.6
Procedure Mapping	

PURPOSE

To provide Pomona College with guidance in developing and implementing the appropriate protective safeguards to support the confidentiality, integrity, and availability of Pomona College assets and information.

POLICY

Pomona College faculty, staff, students, and appropriate third-parties are provided information security awareness education. Pomona College faculty and staff are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, legal requirements, regulations, and agreements. To accomplish this, Pomona College has implemented an information security awareness program that discusses common security shortcomings that can be strengthened through individual action. Pomona College reviews the information security awareness program annually and appropriate updates are applied based on the findings of the annual reviews. Pomona College requires faculty and staff to verify annually that they have completed their information

security awareness training and are aware of their data security responsibilities and Pomona College's information security policies.

GENERAL TRAINING

- Pomona College maintains standard general information security training. This training is used to enhance information security awareness among faculty and staff.
  - General training is also administered:
    - When required by system changes, and
    - As a refresher, general training to faculty and staff on an annual basis.
  - The content of the general training provides users with a basic understanding of the need for information security, actions they need to take to maintain security, information on how to respond to suspected security incidents, as well as the need for operations security.
  - Pomona College includes security awareness training on recognizing and reporting potential indicators of insider threat.
- Due to the different nature of the relationship between Pomona College students and Pomona College faculty and staff, students will be provided with general information security education. This material will be available on the Pomona College ITS website.
  - The student information security education material will differ in certain aspects to that of the faculty staff training.
  - Students are supplied with information security awareness education upon enrollment.
  - Student refresher information security education will be re-administered annually.
- Information security awareness education and training materials and techniques may include tools such as:
  - Displaying posters
  - Offering supplies inscribed with security reminders
  - Generating email advisories or notices
  - Displaying log-on screen messages
  - Conducting information security awareness events
  - Classroom training, or
  - E-learning

PRIVILEGED USER TRAINING[1]

- Pomona College delivers specific role-based training in order to provide access to accounts for authorized users with privileged rights such as:
  - Administrators
  - Super users
  - Sudo, or root level access privileges.
- Privileged users are trained to minimize administrative privileges and only use administrative accounts when they are required.
- Privileged user training includes changing all default passwords before deploying any new applications, operations systems, routers, firewalls, wireless access points, and other systems.
- Privileged user training is provided to authorized individuals prior to them receiving their privileged access. This training is documented and archived.

[1] This standard pertains to system, network, and critical application administrators and/or super users. It does not pertain to users with local administrative rights to their workstation.

- Privileged user training is reviewed annually, upon necessary system changes, and updated accordingly.

THIRD-PARTY TRAINING

- Third-parties, such as suppliers, contractors, and partners, are required to understand their roles and responsibilities regarding Pomona College information security requirements. Depending upon the nature of the third-party relationship, the roles and responsibilities may vary greatly.
- If a third-party has access to sensitive or confidential Pomona College information, the third-party may be required to have in place a training program that meets the same level of requirements as the Pomona College information security training and awareness program.
- In the event that a third-party does not have an adequate information security awareness and training program, Pomona College will administer its training and awareness program for the third-party.

MANAGEMENT TRAINING

- Management and senior leadership have a special role in information security. Management and senior leadership are to be trained on their specific roles and responsibilities with respect to Pomona College information security requirements. Senior leadership is crucial in sponsoring, driving, and supporting the Pomona College information security program.
- Management and senior leadership information security awareness training is administered annually.
- Pomona College maintains a record of management specific training sessions.

SECURITY PERSONNEL TRAINING

- Physical and information security personnel are given specific training based upon their specific roles in the Pomona College information security program.
- Physical and information security personnel are administered role-specific training annually.
- Pomona College maintains records of additional training provided for physical and information security personnel.