# DATA SECURITY POLICY

| | |
|---|---|
| **Policy:** | Data Security |
| **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.DS |
| **NIST SP 800-53 Security Controls** | AC-4, AC-5, AC-6, AU-4, CM-2, CM-8, CP-2, MP-6, PS-3, PS-6, PE-16, PE-19, SC-5, SC-8, SC-10, SC-12, SC-13, SC-17, SC-19, SC-31, SC-28, SI-4, SI-7, SA-10 |
| **NIST SP 800-171 Protecting Controlled Unclassified Information** | 3.1.3, 3.1.4, 3.1.5, 3.4.1, 3.4.7, 3.8.1, 3.8.2, 3.8.3, 3.9.1, 3.9.2, 3.13.11, 3.13.16, 3.14.6, 3.14.7 |
| **Center for Internet Security Critical Security Control** | 1, 2, 13, 14, 18 |
| **Payment Card Industry Data Security Standard (PCI DSS) v3.2** | 1.3, 1.4, 2.4, 3.6, 4.1, 4.2, 4.3, 6.3, 6.5b. 6.6, 6.7 7.1, 7.2, 7.3 |
| **Procedure Mapping** | |
| | |

## PURPOSE

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

## POLICY

Pomona College's information, data, and records are managed in a manner consistent with Pomona College's risk strategy to protect the confidentiality, integrity, and availability of the assets. Data security controls are submitted to Pomona College senior leadership for review and approval, and include a cost-benefit analysis to inform the executive staff in their risk strategy decisions.

## CRYPTOGRAPHY

- The Pomona College system employs cryptographic controls in accordance with applicable Federal and State laws, regulations, and standards
- Pomona College establishes and manages cryptographic keys required for cryptography employed with the Pomona College system in accordance with Federal and State laws, regulations, and guidance
- Pomona College issues public key certificates or obtains key certificates from an approved service provider

## DATA AT REST

- As part of the Pomona College risk assessment process, Pomona College identifies what information at rest warrants encryption and/or other integrity controls. Information at rest refers to the state of information when it is located on a storage device.
- Pomona College system-related information that may require protection includes, but is not limited to:
  - Configuration settings, logs, or rule sets for firewalls and gateways
  - Intrusion detection/prevention system configurations, logs, and related information
  - Router logs and related information, and
  - Authenticator content information, such as password databases
- In alignment with the risk determination, Pomona College protects the confidentiality and integrity of sensitive and confidential data by use of cryptographic mechanisms while the data is stored at rest
  - Pomona College applies full disk encryption to all Pomona College-owned laptops, mobile devices, and desktop workstations
  - Where applicable, Pomona College applies full disk encryption to servers
  - Pomona College backups are encrypted at rest
  - Employs full-device encryption of Pomona College-controlled mobile devices to protect the confidentiality and integrity of the information on Pomona College-controlled mobile devices
    - Please see Bring Your Own Device (BYOD) policy for access control requirements with respect to non-Pomona College-controlled mobile devices
  - Pomona College recommends that students enable full disk encryption on their personal laptops, desktops, and mobile devices.
  - Pomona College-owned transportable media such as backup tapes, USB drives, CD/DVD disks, etc. containing sensitive or confidential data will be encrypted
  - Computer systems and media that employ encryption of data at rest will not have the decryption password stored with the device
- Pomona College may elect to employ additional data at rest controls such as off-line storage and Write-Once-Read-Many (WORM) technologies
- To ensure the security of written information, Pomona College requires:
  - That papers containing confidential information not be left out in public view
  - Papers containing confidential information to be appropriately destroyed when they are no longer needed
  - Printed confidential information to be immediately retrieved from the printer

## DATA IN TRANSIT

- With respect to both internal and external networks and appropriate types of system components, the Pomona College system protects the confidentiality and integrity of transmitted information
- The Pomona College system employs cryptographic mechanisms to prevent the unauthorized disclosure of information and to detect changes to the information during transmission

- The Pomona College system terminates the network connection associated with a communication session at the end of the session or after 10 minutes of inactivity
- Pomona College:
  - Establishes usage restriction and implementation guidance for Voice over Internet Protocol (ViOP) technologies based on the potential to cause damage to the system if used maliciously
  - Authorizes, monitors, and controls the use of VoIP within the Pomona College system

## ASSET HANDLING

- Pomona College documents and manages assets throughout their lifecycle starting with acquisition, and including transfers, removals, culminating in asset disposition
  - Pomona College hardware and software assets are documented, tracked, and managed through the inventory of ITS assets[1]
  - Pomona College faculty and staff status is tracked and managed by Human Resources and the Dean of the College
  - Pomona College student documentation is managed by Admissions, Registrar's Office, the Office of the Dean of Students, and the Advancement Office, depending upon student status
- Pomona College employs sanitization techniques to media prior to disposal and in other instances so as to remove information from the media such that the information cannot be retrieved or reconstructed[2].

## CAPACITY

- Pomona College ensures that there is adequate capacity to provide availability of its system. Pomona College will maintain adequate capacity of resources including, but not limited to:
  - Bandwidth
  - Network
  - Storage
  - Memory
  - Processing resources
  - Electrical power
- Pomona College manages excess capacity to ensure that sufficient capacity is available to counter data flooding attacks
- Pomona College allocates sufficient audit record storage capacity to accommodate the types of auditing performed and the necessary audit processing requirements.

## DATA LOSS PREVENTION

- Pomona College employs reasonable and appropriate controls to prevent data loss. Data loss prevention controls may include, but are not limited to:
  - Monitoring the network for sensitive information, keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across Pomona College network boundaries, and to block such transfers while also alerting information security personnel.
  - Conducting scans of servers to determine whether sensitive data is present on the system in clear text.

---

[1] For further details please see the Pomona College Asset Management Policy
[2] For more details regarding media sanitization, please see the Pomona College Security Operations Policy

- Monitoring all traffic leaving Pomona College and detect for any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices.
- Requiring that confidential information be stored only on Pomona College-controlled system components, storage devices, personally owned devices configured in accordance with the Pomona College Mobile Device policy[3], or third-party storage services

## DATA INTEGRITY

- Pomona College utilizes integrity checking mechanisms to detect unauthorized changes to Pomona College hardware software, firmware, and information. Unauthorized changes to hardware software, firmware, and information can occur due to errors or malicious activity.
- Pomona College systems perform integrity checks of hardware software, firmware, and information
  - Periodically
  - Upon occurrence of a security related event such as:
    - Identification of a new threat to which Pomona College is susceptible
    - Installation of new hardware
    - Installation of new software
    - Installation of new firmware
  - Upon entering a transitional state, such as:
    - System startup
    - Restart
    - Shutdown
- Pomona College incorporates the detection of unauthorized changes to the system into the incident response process

## DEVELOPMENT ENVIRONMENT

- Where applicable, Pomona College maintains a baseline configuration for system development and test environments that is managed separately from the Pomona College production baseline configuration.
  - Establishing separate baseline configurations for development, testing, and production environments helps Pomona College protect its system from unplanned and unexpected events related to development and testing activities.
  - Separate baseline configurations allow Pomona College to apply configuration management that is most appropriate for reach type of configuration.

[3] See Pomona College Mobile Device policy