MOBILE DEVICE POLICY

Policy:	Mobile Device
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)	ID.AM-4, PR.AC-3
NIST SP 800-53 Security Controls	AC-19, AC-20
NIST SP 800-171 Protecting Controlled Unclassified Information	3.1.18, 3.1.19, 3.1.20, 3.1.21
Center for Internet Security Critical Security Control	5, 12, 15
Payment Card Industry Data Security Standard (PCI DSS) v3.2	4.1, 5.1, 5.2, 5.3, 5.4, 11.1
Procedure Mapping	

PURPOSE

To provide guidance to Pomona College, Faculty, and Staff on the appropriate use of both College-issued and personally-owned mobile Devices containing or accessing Pomona College confidential information.

POLICY

Mobile Devices are an effective and necessary business tool for many employees; however, their use presents risks to employees, individually, and to Pomona College. In order to protect against such risks, Pomona College requires all employees with authorized access to Pomona College confidential information who use mobile Devices in connection with their jobs to follow the requirements of this Policy.

This Policy applies to all Pomona College employees in their use of mobile devices (Devices), including but not limited to wireless phones, smartphones, tablet computers or other mobile e-mail. Pomona College owns and issues Devices to eligible employees and permits employees to use their own personal Devices which meet standards for Pomona College business purposes. This Policy governs the use of any such Device, including both College-issued Devices and personally-owned Devices**,** for any Pomona College related business purpose**.**

Since Devices can be used to access Pomona College networks, systems and data, their use presents significant risks to the security of Pomona College data (hereafter, “College Data”). College Data includes any Pomona College related information, emails, documents, pictures, video, recordings or data

whatsoever (including student data), whether or not such data is classified as confidential. In order to protect College Data and ensure compliance with data privacy laws, Pomona College requires all Devices (*including personal Devices used to access Pomona College networks or data)* to comply with certain minimum security standards as detailed below ("Security Standards"). It is the responsibility of the user to ensure that their device complies the Security Standards detailed below prior to accessing the Pomona College networks or data.

POMONA COLLEGE-ISSUED DEVICES

Pomona College-issued Devices are intended to be used for Pomona College educational and business purposes. Eligibility for a College-issued Device is based on consideration of the employee's educational or business needs, and requires approval by the head of his/her department. The types of College-issued Devices are limited based on the Security Standards and other business requirements. Requests for the issuance of a device to an eligible employee must be formally approved by employee's manager submitting a device requisition to Pomona College ITS.

Employees will not be billed for their use of Devices issued by the College and used in accordance with this Policy. The costs for the Devices and the wireless services, when applicable, will be billed to Pomona College and charged to the Employee's cost center. Only Devices that have been approved by Pomona College and that meet the Security Standards can be issued to employees under this Policy.

All Devices provided by Pomona College are the property of Pomona College and may be periodically replaced or upgraded as determined and processed by Pomona College. Employees may not upgrade or replace their Devices on their own. Procurement of new Devices must be processed through ITS unless otherwise approved. Such Devices must be returned to Pomona College upon termination or resignation of employment, or upon notification by Pomona College for any reason.

PERSONALLY-OWNED DEVICES

Employees may use their own personal Devices for Pomona College purposes, provided that they are in compliance with all requirements of this Policy. Employees must comply with the Security Standards and all other requirements of this Policy at all times.
If an employee uses a personal Device that is not compliant with Pomona College' Security Standards, that Device should not be used to receive, store or transmit Pomona College Data. Non-compliant Devices should not be used to access to Pomona College's networks or systems. Any use of such Devices by an employee to obtain access to College Data will be a violation of this Policy.

SECURITY STANDARDS FOR ALL DEVICES

College-issued and personally-owned Devices used for any Pomona College purpose must meet or exceed the following Security Standards:

- Protected logon, which may be either:
  - A password or PIN with a minimum of 6 characters
  - Fingerprint
  - Authenticating pattern
- Device screen automatically locks after 5 minutes of inactivity
- Device Encryption
- Pomona-owned devices must permit central management by ITS

USER SECURITY AND SAFETY

All Device users must maintain and comply with the above Security Standards on their Devices at all times. Employees are encouraged to use Pomona provided services for storing College data whenever possible, preferably minimizing the amount of data stored on their personal device, thus minimizing the

chance of lost or stolen data that may result in a breach. College Data should be stored only on secure Pomona College managed databases, and should not be transmitted or backed up to sources that are not secure or Pomona College managed.

Faculty and Staff must immediately report to their managers and ITS the loss or theft of their Device or any other potential security compromise involving their Device. Upon such occurrence, Pomona College is to cause the remote wiping of all data on Pomona-owned devices. For employee-owned devices, the employee is encouraged to remotely wipe their device.

In addition, safety must be the first priority at all times when using a Device. It is widely acknowledged that the use of mobile Devices while driving can significantly increase the risk of accidents. In California, the use of handheld Devices while operating a motor vehicle is illegal. When traveling, employees are expected to be familiar with the laws and ordinances in the states in which they operate motor vehicles. Under no circumstances are employees allowed to place themselves at risk to fulfill College needs. Employees are strongly encouraged to refrain from using a mobile phone while driving. Text messaging or reading or writing emails while driving is not appropriate under any circumstance.

Any use of programs or tools for "rooting", "jail breaking" or to bypass or override the Security Standards is deemed a violation of this Policy.

USE OF THE DEVICES

Employees must comply at all times with all applicable laws and all Pomona College policies (including but not limited to the Appropriate Use Policy) in the use of their Devices. College-issued Devices are to be used primarily for educational and business purposes for the benefit of Pomona College. Personal use of such Devices is allowed, but should be within reasonable limits. Employees are personally responsible for any charges incurred related to non- business applications, games, ringtones, etc.

DEVICE DISPOSAL, UPGRADES, OR RECYCLING

Faculty and Staff who have Pomona College information on their device need to follow secure and legally-compliant means of disposing of their Devices. Employees who wish to upgrade their Device need to ensure that their existing Devices are disposed of in a secure and legally-compliant manner. College-issued Devices must be returned to ITS to complete the upgrade process. Upgrade Devices are also subject to this Policy in all respects. Employees may not participate in third party recycling programs with their College-issued or personally-owned Devices without first wiping all College Data from the Device. Please consult with Pomona College ITS, who can assist in data wiping of Devices in preparation for disposal and/or upgrade.

EMPLOYEE TERMINATION

In the event of termination of employment or resignation, College-issued Devices must be immediately returned to Pomona College. Employees are responsible to remove any College Data from personally-owned Devices immediately upon termination or resignation. College-issued Devices are subject to remote wiping. Employees will be responsible for all charges related to the replacement of Devices for non-returned Devices. Employees with College-issued devices will be personally liable for charges of any kind incurred after their date of termination or resignation. Phone numbers on College-issued Devices remain Pomona College property and will not be released to employees leaving the College.