PimaCountyCommunityCollegeDistrict
Administrative Procedure

AP Title:	**College-Issued Mobile Device Security**
AP Number:	AP 9.01.04
Adoption Date:	11/13/06
Schedule for Review & Update:	Every two years
Review Date(s):	2/7/12, 6/2/15, 5/20/21
Revision Date(s):	5/20/21
Sponsoring Unit/Department:	Information Technology
Policy Title(s) & No(s).:	Information Technology Resource Management, BP 9.01
Legal Reference:	
Cross Reference:	College Employees Personnel Policy Statement, Appendix E

PURPOSE

This AP outlines a set of practices and minimum requirements for the safe use and management of College-issued mobile devices. This AP applies to all College-issued mobile devices, including the devices already issued to authorized College users.

SECTION 1: Definitions

"AP" means Administrative Procedure.

"Cloud Services" mean such service models as defined within NIST SP800-145, further included within FedRAMP v.4.2 at p.3, as are used by, connected to, or communicate with Mobile Devices as defined, whether the Cloud Services are provided by the College or accessed for personal use.

"Mobile Devices" include, but is not limited to, removable storage devices (e.g., USB flash drives, external hard drives), portable communications and computing devices (e.g., laptops, notebooks, tablets, PDAs, telephones, wearable devices, and Wi-Fi "Hotspots"), and other similar devices.

SECTION 2: Procedure and Responsibilities

2.1 Acceptable Use of College-Issued Mobile Devices

2.1.1 College-issued Mobile Devices are intended to be used solely for official College related purposes, including, but not limited to, a) as a primary computing device on a College campus or other College property; b) as the user's primary or alternative device while performing College-related tasks at a non-College location or traveling on official College business, or c) any other College related tasks.

2.1.2 College-issued Mobile Devices should not be used by anyone other than the specific user to whom the device was issued.

2.1.3 Incidental personal use of College-issued Mobile Devices is permitted, provided that such use does not interfere with or detract from College operations, including but not limited to employee work performance, and is otherwise consistent with this AP and other applicable College policies and procedures.

2.1.4 Users of College-issued Mobile Devices may be required to reimburse the College for any usage resulting in unauthorized charges to the College, regardless of whether such charges were sustained during use of the Mobile Device for official College business or for personal purposes.

2.2 Privacy Expectations

All College-issued Mobile Devices, and any information or data contained on them, remain the sole and exclusive property of the College at all times. Users of College-issued Mobile Devices do not have a right, nor should they have an expectation, of privacy while using College-issued mobile devices at any time, including accessing the Internet and using e-mail, Cloud Services, and voice communications. By acceptance of the College-issued mobile device, users consent to disclosure and/or monitoring of device usage, including the contents of any files or information maintained, processed, or passed-through that device.

2.3 Responsibilities of Users of College-Issued Mobile Device

2.3.1 Each user of a College-issued Mobile Device is responsible for the safekeeping and care of the assigned device. If the College-issued Mobile Device is damaged, lost, or stolen, the user must immediately report it to the issuing department.

2.3.2 Upon resignation, retirement, withdrawal, graduation, or other separation from the College, users must return all College-issued Mobile Devices and all accompanying accessories to the issuing department on or before their final day with the College or at another date specified by the issuing department. Failure to timely return College-issued Mobile Device will result in cost-recovery measures by the College, including, but not limited to withholding money from final paychecks or placing holds on students accounts. The College likewise reserves the right to report unreturned College-issued Mobile Devises to the police as unlawfully retained or stolen property.

2.4 Security

2.4.1 All College-issued Mobile Devices must be enrolled into the College's mobile device management program at all times.

2.4.2 All College-issued Mobile Devices that access or store sensitive, confidential, or personally-identifiable information must be encrypted.

2.4.3 All College-issued Mobile Devices, where possible, must be secured using a PIN or other password protection.

2.4.4 All College-issued Mobile Devices must be kept up to date with the latest security patches, virus-scanning software and virus data files, and end-point security agent(s.)

2.4.5 All College-issued Mobile Devices, where possible, must have remote data wipe capability installed and enabled. The data will be wiped from the mobile devices, either directly or remotely, in the following circumstances:

- Whenever the mobile device is reported lost, stolen, or compromised

- After ten (10) consecutive failed password attempts
- Whenever the College IT detects a data breach, a virus or similar threat to the security of the College data, Cloud Service(s,) and technology infrastructure
- Before transferring possession of a mobile device from one College employee to another
- Before disposing of the mobile device
- When necessary for servicing as required by the manufacturer, or College-directed operating procedures, or at service intervals prescribed by the College or manufacturer.

2.4.6 The security protections for College-issued mobile devices will be reviewed at least annually.

2.5 Enforcement

Non-compliance with this AP may result in disciplinary action and/or revocation of College-issued Mobile Devices.

2.6 Authority

2.6.1 The Assistant Vice Chancellor for Information Technology is responsible for implementing and overseeing compliance with this AP.

2.6.2 Before issuing a Mobile Device, the Assistant Vice Chancellor for Information Technology or designee shall require the recipient to sign a Mobile Device Agreement. The Assistant Vice Chancellor for Information Technology or designee shall maintain a record of all Mobile Device Agreements.