8045.S400 Mobile Device Management

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

Introduction

Campuses must implement controls designed to protect CSU resources that are accessed from or stored on mobile devices.

1.0 Mobile Device Management

As determined necessary by risk assessment, mobile devices must be protected with appropriate security controls. Appropriate security controls can include, but are not limited to:

a) Access control
b) Encryption
c) Strong passwords
d) Anti-virus software
e) Personal firewall

2.0 Storage of Protected Data

2.1 Protected Level 1 data may not be stored on a mobile device unless authorized by appropriate campus administration and encrypted via campus-approved method.

2.2 Each campus must maintain a current inventory of mobile devices that contain protected Level 1 data. This inventory must be reviewed at least annually.

3.0 User Practices for Mobile Devices

3.1 Campuses must identify and communicate approved user practices for mobile device security. Campuses must provide these practices to any individual issued a campus-provided mobile device and include information about mobile device security in security and awareness training material for all campus users.

3.2 Campuses must maintain and publish and a process for users to report if they determine or suspect that any mobile device (including those not provided by campus) which enables access to non-public campus information assets has been lost, stolen, or compromised.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
10/8/11	Macklin	Incorporation of ISAC and NTA comments	All
11/9/2011	Moske	Formatted	All
1/12/2012	Macklin	Final Review	None
2/19/2013	Macklin	ISAC Review/Approved	3.0, 4.0

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
2/19/13	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for posting