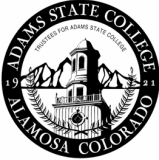


<u>ADMINISTRATIVE POLICY</u>  ADAMS STATE COLLEGE	POLICY NUMBER: 500-004	PAGE NUMBER Page 1 of 3
	CHAPTER: Computing Services	
	SUBJECT: Mobile Computing Policy	
RELATED POLICIES: ASC Trustee Policy Manual : Section 7.1: Duties and Responsibilities of the College President...(in part) The President is also expected to ensure that the policies, procedures and actions of the Board are communicated to appropriate constituencies of the College in a timely manner. OFFICE OF PRIMARY RESPONSIBILITY: Computing Services	EFFECTIVE DATE: 01 June 2007	
	SUPERSESSION:	
	Dr. David Svaldi President	

I. POLICY

- A. The use of mobile computing devices and mobile storage media increase security risks via loss, theft, unauthorized access, malware, and remote data transfer and need to be secured to protect the information resources of Adams State College (ASC).
- B. Sensitive data storage: Mobile computing devices or storage media that contain sensitive data must use ASC approved encrypted storage methods.
- C. Sensitive data transfer: Transfer of sensitive data must use ASC approved encrypted transfer methods.
- D. Device security: Mobile devices used to access or store sensitive data must comply with ASC standards for protection against unauthorized access and malware.
- E. Audit: Mobile computing devices, storage media, and data transfers are subject to various types of security audit by ASC Computing Services.
- F. Network access: Use of mobile computing devices connecting to the ASC network is further governed by all other ASC policies and procedures, as well as applicable local, state, and federal laws.
- G. Physical security: ASC standards will be followed to physically secure mobile devices.

II. PURPOSE

- A. The purpose of this policy is to establish security standards for mobile computing and storage devices that contain or access information resources at ASC.
- B. Sensitive data storage: Encrypted storage reduces risk due to loss or unauthorized access to a mobile devices or media.
- C. Sensitive data transfer: Encryption reduces risk of exposing data during transfer.
- D. Device security: Increases difficulty of unauthorized access to a mobile device.

CHAPTER:	SUBJECT	POLICY #	Page 2 of 3
Computing Services	Mobile Computing Policy	500-004	EFFECTIVE 01 June 2007

- E. Audit: Increase compliance with ASC policies.
- F. Physical security: Reduce theft, loss and other physical damage to mobile devices and media.

III. DEFINITIONS

- A. Sensitive data: Data deemed restricted, protected, or private by ASC policy or local, state, or federal laws.
- B. Mobile computing device: Any portable device that provides computing or information storage and retrieval capabilities, including but not limited to laptop computers, PDA's, cell phones, flash drives, and portable hard drives.
- C. Mobile storage media: Any medium used to store electronic data, including but not limited to CD's, DVD's, tapes, and diskettes.
- D. Encryption: Conversion of data into a form called a ciphertext, that cannot be easily understood by unauthorized people.
- E. Malware: Refers to any software designed to cause damage to a computing device.

IV. PROCEDURES

- A. Loss or theft: Report loss of any computing device or storage media to Computing Services.
- B. Approved encryption methods: ASC Computing Services will maintain and provide a list of products, methods, and relevant instructions to facilitate approved encrypted data storage and transfer.
- C. Audit: Computing Services may audit any mobile device connected to the ASC network, and any data transfer taking place on, to, or from the ASC network to check for unsecured sensitive data and unsecured devices.
 - 1. Most audits will be automated and designed to minimize disruption of day to day academic and business processes.
 - 2. Audits of ASC owned mobile computing devices and mobile storage media by Computing Services personnel may be scheduled and could prevent use of the mobile device or media during the audit.
 - 3. If a device, media or transfer is found to be unsecured or contain unsecured sensitive data, reasonable attempt will be made to contact and work with the relevant ASC personnel to bring the device or transfer into compliance.
 - 4. Computing Services may disable a device or transfer if contact cannot be made with relevant personnel in a reasonable amount of time or the severity of exposure to unauthorized device access or sensitive data leakage merits immediate action.
- D. Reporting: ASC must comply with local, state, and federal laws pertaining to loss, exposure, or potential exposure of sensitive data. These laws may require timely public disclosure about the data and direct notification of people the data pertains to.
- E. Physical security: ASC Computing Services will maintain and provide a list of products, methods, and relevant instructions to facilitate approved physical security of mobile devices and media.

CHAPTER:	SUBJECT	POLICY #	Page 3 of 3
Computing Services	Mobile Computing Policy	500-004	EFFECTIVE 01 June 2007

V. RESPONSIBILITY

Responsibility for implementation of this policy falls on the ASC Computing Services Department and ASC personnel who use mobile computing devices or handle sensitive data.

VI. AUTHORITY

This policy has been prepared under the authority of the President, Adams State College, as delegated by the ASC Board of Trustees.

VII. HISTORY

VIII. ATTACHMENTS