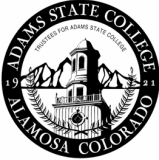


<u>ADMINISTRATIVE POLICY</u>  ADAMS STATE COLLEGE	POLICY NUMBER: 500-05	PAGE NUMBER Page 1 of 4
	CHAPTER: Computing Services	
	SUBJECT: Data Handling and Storage Policy	
RELATED POLICIES: ASC Trustee Policy Manual : Section 7.1: Duties and Responsibilities of the College President...(in part) The President 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: 1 August 2007	
	SUPERSESION: 00/00/00	
	Dr. David Svaldi President	

I. POLICY

Institutional data is information that supports the mission of Adams State College. It is a vital asset and is owned by the College. Institutional data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth the college's standards with regard to the handling of sensitive institutional data.

II. PURPOSE

To establish policy for the safeguarding of restricted and sensitive data relating to students and ASC personnel that is created, received, maintained or transmitted by the College. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all college policies and applicable state and federal laws. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.

III. DEFINITIONS

A. Archiving/Storage: The act of physically or electronically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.

B. Institutional Data: Institutional data is information that supports the mission of Adams State College. It is a vital asset and is owned by the College. Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with established institutional policies and practices. Sensitive Data as defined in this section is a subset of Institutional Data.

C. Authorized User: Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include, but are not limited to faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of the college.

D. Electronic Media: All media on which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs and USB storage devices.

E. Electronic Messaging: A set of communication processes used to relay information among the users of computers. Electronic Messages take many forms. Examples: Electronic Mail (E-Mail), FTP, cell phones, Instant Messaging and internet chat.

F. Restricted Data: Data whose access is restricted by federal or state statute (i.e. HIPPA, FERPA). For purposes of this policy, restricted data is a subset of sensitive data.

G. Sensitive Data: Data, regardless of its physical form or characteristics, with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination because it contains information which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the college or compromise public activities. Examples include: passwords, intellectual property, on-going legal investigations, medical or grades information protected by FERPA or HIPAA, social security numbers, birth dates, professional research, graduate student work, bank or credit card account numbers, income and credit history.

CHAPTER:	SUBJECT	POLICY #	Page 2 of 4
Computing Services	Data Handling & Storage Policy	500-05	EFFECTIVE 1 August 2007

IV. DATA COLLECTION

- A. Users should collect only the minimum necessary institutional/sensitive information required to perform college business.
- B. Department heads must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with college policy and procedure.

V. DATA ACCESS

- A. Only authorized users may access, or attempt to access, sensitive information.
- B. Authorization for access to sensitive data comes from the department head, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other official authority.
- C. Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform college business.
- D. Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- E. Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the ASC Computing Services department.

VI. DATA HANDLING AND DATA TRANSFER

- A. Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.
- B. Sensitive data must be protected from unintended access by unauthorized users. Users must guard against unauthorized viewing of such information which is displayed on the user's computer screen. Users must not leave sensitive information unattended and accessible.
- C. Sensitive information must not be taken off-campus unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.
- D. Sensitive data should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.
- E. Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive or laptop.

VII. STORAGE OF SENSITIVE DATA

- A. Physical protection must be employed for all devices storing sensitive data. This shall include physical access controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.
- B. Users of lap-top and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the College.
- C. Computing Services managed servers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.
- D. Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.
- E. It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system should be stored on a network drive hosted on a Computing Services managed server.

CHAPTER:	SUBJECT	POLICY #	Page 3 of 4
Computing Services	Data Handling & Storage Policy	500-05	EFFECTIVE 1 August 2007

F. Electronic media storing restricted/sensitive data must be protected by password security. To the extent possible, these devices must employ encryption methods.

VIII. DATA RETENTION AND DISPOSAL

A. Retention of Records Containing Restricted and Sensitive data: A “schedule” describing the records and the official retention period is required by the state of Colorado for each type of record created or maintained by a public institution. Adams State College uses the following guidelines and statutory procedures for records retention.

1. The Colorado State Archives Records Management Manual, with particular attention to Higher Education Agencies (Part I – Schedule 8) “General Records Retention Schedules For Community Colleges, State Colleges and Universities”
2. CRS 24-80-101 to 24- 80-111 (Public Records Law)

B. Archiving: Institutional records, including sensitive information records, which are not being used for active college business, may be archived until retention requirements have been met.

1. Departments determine the criteria for inactive record status in their areas, based on need for the records and available storage space and public records law.
2. Storage areas for inactive records must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.
3. When appropriate, only primary student records should be archived. The contents of true “Shadow” records should be destroyed after it has been determined that they contain only duplicates of records maintained elsewhere, and do not contain any original materials.
4. Off-site storage facilities or locations for sensitive records must be approved by the Records Management Office.

C. Record Disposal: The proper destruction of public records is essential to creating a credible records management program. Records containing restricted/sensitive data shall only be destroyed in the ordinary course of business; no records that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.

1. No primary records of any type belonging to Adams State College may be destroyed until they have met retention requirements established by ASC policies and public records law.
2. When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction later.
3. The authorized methods of destruction for non-electronic records are burning where authorized or shredding. The authorized methods of destruction for electronic records are wiping or physical destruction of the electronic media, and where possible, to utilize the US Department of Defense standard for clearing and sanitizing electronic media: DOD 5220.22-M.

IX. RESPONSIBILITY

A. Supervisory Personnel: Every ASC employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for the following:

1. Communicating this policy to personnel under their supervision.
2. Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.
3. Providing education and training in data management principles to employees under their supervision.

B. User Responsibilities: Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

1. Access institutional/sensitive data only in their conduct of college business.

CHAPTER:	SUBJECT	POLICY #	Page 4 of 4
Computing Services	Data Handling & Storage Policy	500-05	EFFECTIVE 1 August 2007

2. Request only the minimum necessary confidential/sensitive information necessary to perform college business
3. Respect the confidentiality and privacy of individuals whose records they may access.
4. Observe any ethical restrictions that apply to data to which they have access.
5. Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

X. COMPLIANCE

Compliance with this data protection policy is the responsibility of all members of the Adams State College community. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to ASC's information technology resources during investigation of an alleged abuse. Violations can also be subject to prosecution by state and federal authorities.

XI. AUTHORITY

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

XII. HISTORY

XIII. ATTACHMENTS