


| | | |
|--|---|----------------------------|
| <u>ADMINISTRATIVE POLICY</u>  ADAMS STATE COLLEGE | POLICY NUMBER: 500-006 | PAGE NUMBER Page 1 of 3 |
| | CHAPTER: Computing Services | |
| | SUBJECT: Information Technology (IT) User Responsibility 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 May 2008 | |
| | SUPERSESSSION: | |
| | Dr. David Svaldi President | |

I. PURPOSE

- A. This policy establishes the basic Information Technology (IT) security safeguards that must be taken by every person using an Adams State College (ASC) IT resource or otherwise accessing College information. More detailed IT policies are referenced in section III of this document. Additional safeguards may be appropriate, depending on the situation and its inherent risk to ASC information and IT resources.
- B. This policy does not impose restrictions that are contrary to ASC's established culture of sharing, openness, and trust. However, the College is committed to implementing the safeguards necessary to ensure the privacy of personal information, the availability of College information and IT resources, and the integrity of ASC's operations.

II. POLICY

- C. It is the responsibility of every IT resource user to know the College's IT security requirements and to conduct her/his activities accordingly. IT resource users shall comply with the following requirements:
 1. **Protect the Privacy of Others.** Users shall respect the privacy of others when handling personal information and shall take appropriate precautions to protect that information from unauthorized disclosure or use.
 2. **Do Not Store Sensitive Information on Workstations and Mobile Devices, Except When Specifically Needed for Business Purposes.** Ordinarily, sensitive information shall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and appropriately secured. If sensitive information is stored on a workstation or mobile computing device or transmitted to an external network or organization, IT resource users shall encrypt or adequately protect that information from disclosure. In addition to encryption, other protections may include the use of passwords, automatic logoffs, and secure Internet transmissions. The protection of sensitive information shall be in accordance with campus IT security requirements and other guidance as available from ASC's Computing Services Department.
 3. **Keep a Clear Desk and Clear Computer Screen.** IT resource users shall keep all sensitive information out of plain sight unless in use and shall not leave such information displayed when it is not needed.
 4. **Protect Workstations and Other Computing Devices.** IT resource users are responsible for helping to maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g., viruses, worms, and spyware). Users shall consult ASC's Computing Services Department for guidance on protecting their computing devices.

| CHAPTER: | SUBJECT | POLICY # | Page |
|--------------------|-------------------------------|----------|--------------------------|
| Computing Services | IT User Responsibility Policy | 500-006 | EFFECTIVE 01 May 2008 |

5. **Protect Passwords.** Passwords are used to authenticate the identity of individuals and gain access to College resources. Each person is responsible for protecting the passwords assigned to her or him and shall not share them with others.
6. **Report Security Violations, Malfunctions, and Weaknesses.** IT resource users shall report security related events; known or suspected violations of IT security policy; and inappropriate, unethical, and illegal activities involving College IT resources to ASC's Computing Services Department.
7. **Utilize University Information and IT Resources for Authorized Purposes Only.** IT resource users shall access or otherwise utilize College information and IT resources only for those activities they are specifically authorized and in a manner consistent with ASC's policies, federal and state laws, and other applicable requirements.

III. RELATED IT POLICIES

- A. The following policies provide detailed information relating to the roles and responsibilities of the ASC computing community. Users of campus IT resources are responsible for reading and complying with these policies. These policies may be found on the ASC Computing Services Web Site, <http://www2.adams.edu/administration/computing/>. Questions regarding these policies should be directed to ASC's Chief Information Officer.
 1. Policy 500-001, ASC Bandwidth Policy
 2. Policy 500-002, ASC Voicemail Policy
 3. Policy 500-003, Acceptable Use Policy
 4. Policy 500-004, Mobile Computing Policy
 5. Policy 500-005, Data Handling & Storage Policy

IV. COMPLIANCE

Compliance with this policy and those IT-related policies referenced in Paragraph III is the responsibility of all members of the Adams State College IT community. Violations of 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.

V. RESPONSIBILITY

Responsibility for implementation of this policy falls on the ASC Computing Services Department and ASC IT resource users.

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

Amended: Original Policy; Approved 16 April 2008

Initial Policy Effective: 1 May 2008

Supersedes: N/A

VIII. ATTACHMENTS

Not Applicable