ADMINISTRATIVE POLICY ADAMS STATE COLLEGE	POLICY NUMBER: 500-007	PAGE NUMBER Page 1of 3
	CHAPTER: Computing Services	
	SUBJECT: IT Administrator Access 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: 29 January 2009	
	SUPERSESSION:	
	Dr. David Svaldi President	

I. POLICY

A. This document defines Adams State College's (ASC's) policy regarding the granting of local Administrator rights on College owned computer workstations.

B. By default, all ASC Faculty & Staff members are assigned General access level rights on their individual (local) workstations. Exceptions may be granted by the ASC Chief Information Officer (CIO) for those individuals who require Administrator level access to perform job related tasks.

II. PURPOSE

A. Local Administrator level access allows the computer user to have complete and unrestricted access to their computers, increasing overall campus IT security risks.

B. The purpose of this policy is to ensure that local Administrator access is only granted when needed for institutional related functions and is done so in a deliberate and thoughtful manner.

C. Individuals may request Administrator level access by submitting the Request for Workstation Administrator Access Form provided as an Attachment to this Policy.

D. Administrator Guidelines: Individuals granted Administrator access incur increased responsibility to safeguard ASC's computer network through diligent adherence to the following guidelines, in conjunction with those addressed in the IT policies summarized in Paragraph IV of this document.

1. Individuals should only install software on their workstations that is related to college business
2. Individuals should not install software that may damage files and expose ASC's network to virus attacks and malicious coding
3. Individuals should not install software applications that degrade network performance or cause noticeable system slowdowns across wide areas of the campus
4. Individuals should not download or install software applications that are illegal or not licensed on college owned equipment
5. Individuals who download or install applications, other than those included in the standard configuration for all college computers, are responsible for retaining documentation of appropriate licenses.

E. Support Guidelines: Workstations that contain non-standard campus software pose special support problems for Computing Services. Accordingly, the following support guidelines will be followed by Computing Services when working on computer's used by personnel who have been granted Administrator access.

1. Non-standard software will be removed as part of a normal repair process if necessary to restore system functionality. However, no software will be removed without fully coordinating its removal with the workstation user.
2. In the event of computer or network performance issues associated with a computer enabled with Administrator level access, Computing Services will only restore the computer to the standard configuration for all ASC computers. Before the computer is "re-cloned" to the standard configuration, this action will be coordinated with the workstation user.
3. The occurrence of repeated instances of computer integrity problems may result in the removal of Administrator level access in order to prevent increased IT security risks to the campus and continued challenges in supporting the computer

III. DEFINITIONS

A. Administrator Access Level: Allows the user to have complete and unrestricted access to the computer. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts and change file level permissions. Manipulating these may cause serious system stability issues and system vulnerabilities

B. General Access Level: Allows most administrative powers with some restrictions. Installation of software or hardware that makes changes to the underlying operating system will require the assistance of Computing Services. General Access Level will generally assure the highest level of stability for a computer.

IV. RELATED IT POLICIES

B. 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
6. Policy 500-006, IT User Responsibility

V. COMPLIANCE

Compliance with this policy and those IT-related policies referenced in Paragraph IV 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.

VI. RESPONSIBILITY

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

VII. AUTHORITY

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

VIII. HISTORY

Initial Policy Effective: 29 January 2009

Supersedes: N/A

IX. ATTACHMENTS

A. Request for Workstation Administrator Access Form