Section 1	**Information Technology Services**	1/28/2009	-Effective
		1/28/2009	-Revised
Policy 1.0 – 1.6	**Change Management**	ITS	-Author

1. CHANGE MANAGEMENT

1.1. Introduction

The Information Technology (IT) infrastructure at Amarillo College (AC) is expanding and continuously becoming more complex. There are more constituencies dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Technology Services (ITS) and the AC community grows, the need for a strong change management process is essential.

Each ITS element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unscheduled or emergency outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable IT resource infrastructure.

1.2. Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that AC employees can plan accordingly. Changes require serious forethought, planned implementation, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of IT resources.

1.3. Audience

The Change Management Policy applies to any individuals who initiate or participate in changes to IT resources.

1.4. Definitions

1.4.1. **IT resources include** any and all technology-based systems owned by or licensed to AC that are capable of creating, printing, storing, and displaying information and used to perform AC work. This includes computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology, telecommunication resources,

network environments, telephones, fax machines, printers, wireless antennae, smart classroom and instructional devices such as projectors, document cameras, and DVD players).

1.4.2. Additionally, IT resources include the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

1.4.3. **Owner** includes any manager or agent upon whom responsibility rests for carrying out the program or function that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

1.4.4. **Custodian or Guardian** or caretaker is the provider of services who is charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For example, ITS is the custodian for administrative applications; for micro and mini-applications the owner or user may retain custodial responsibilities. Normally, the custodian is a provider of services.

1.4.5. **Change Management** is the process of controlling modifications to hardware, software, firmware, and documentation to ensure that IT resources are protected against improper modification before, during, and after system implementation and to ensure minimum disruption of the business processes of the institution.

1.4.6. **General Maintenance** is not covered by the change management policy and may include minor modification to existing systems or applications such as software updates within a version, reimaging computers, basic maintenance of computers and/or AV systems.

1.4.7. **Change includes** any modifications to hardware or software that have the potential to interrupt service, alter functionality, or provide new technology capability.

1.4.8. **Scheduled Change** occurs when formal notification has been received, reviewed, and approved through the review process in advance of the change being made.

1.4.9. **Unscheduled Change** is a change which occurs in the absence of notification via the formal process in advance of the change being made, and will only be acceptable if based on maintaining system integrity and security in a timely manner to prevent an emergency situation.

1.4.10. **Emergency Change** may occur when an immediate response to imminent critical system failure is needed to prevent widespread service disruption, such as a system failure, security breach, or data corruption.

1.5. Change Management Policy

1.5.1. Every change to a IT resource, including operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

1.5.2. The Information Technology Council (IT Council) will serve as a Change Management Committee and will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.

1.5.3. All changes or modifications to IT systems, networks, programs or data must be approved by the owner department that is responsible for resource integrity.

1.5.4. A formal, written Change Request Form must be submitted to the IT Council for all changes, both scheduled and unscheduled.

1.5.5. All scheduled change requests must be submitted in accordance with change management procedures so that the IT Council has time to review the request, determine and review potential concerns, and make the decision to allow or delay the request.

1.5.6. Each scheduled change request must receive formal IT Council approval before proceeding with the change.

1.5.7. The Change Request Form must include the following information:

1.5.7.1. Date of Submission

1.5.7.2. Anticipated Date of Change

1.5.7.3. Owner Contact Information

1.5.7.4. Custodian Contact Information

1.5.7.5. Nature of the Change

1.5.7.6. Purpose of the Change

1.5.7.7. Description of the Change and anticipated time frame for Change implementation

1.5.7.8. Affected audience, including campuses, departments, groups, individuals

1.5.7.9. Testing/piloting procedures, as necessary

1.5.7.10. Possible back-out procedures if problems should occur during implementation

1.5.7.11. Announcement message to affected populations which will be distributed 48 hours prior to implementation

1.5.8. The IT Council may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change would negatively impact a key business process such as year-end accounting, or adequacy of available resources. Adequate resources may be a problem on weekends, holidays, or during special events.

1.5.9. Owner and custodian notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures below.

1.5.10. A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.

1.5.11. A Change Management Log must be maintained for all changes and submitted to the IT Council when the change is completed. The log must contain, but is not limited to:

a) Date of submission
b) Date of change
c) Owner and custodian contact information
d) Nature of the change
e) Purpose for the change
f) Indication of success or failure

1.5.12. All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the CIO, the IT Council, and the Physical Plant.

1.6. References

The State of Texas Information Act
http://www.tsl.state.tx.us/slrm/recordspubs/stbull04.html

Texas Government Code, Section 441
http://www.tsl.state.tx.us/agency/customer/pia.html

Texas Administrative Code, Chapter 202
http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202

IRM Act, 2054.075(b)
http://www.dir.state.tx.us/oversight/

The State of Texas Penal Code, Chapters 33 and 33A

DIR Practices for Protecting Information Resources Assets

DIR Standards Review and Recommendations Publications