Policy Under IT Council Review (April 2009)

Disciplinary Actions (1.8) deferred pursuant to IT Council discussion/action.
Status: Accepting edits from the IT Council

Section 4	**ITS Policies**	mm/dd/yy	-Effective
		3/31/09	-Revised
Section	**Data Access and Information Security**	Info Tech Serv.	-Author

1. DATA ACCESS AND INFORMATION SECURITY

1.1. Introduction

The Amarillo College (AC) Information Technology Services (ITS) network serves as the primary repository of institutional, academic, employee and student data. It is the responsibility of all AC employees to protect and secure all institutional data.

1.2. Purpose

The purpose of the policy is to assure data integrity and confidentiality of all institutional data, as well as control access and educate users regarding limitations and liabilities pertaining to data access.

1.3. Audience

This policy is for all AC employees that have access to data.

1.4. Definitions

1.4.1. **Electronic data** includes any data stored in personnel or student records, institutional data used for institutional research, academic program information and any data deemed sensitive by AC supervisors, managers, or executive level leaders.

1.4.2. **Electronic storage media** includes but is not limited to any device capable of storing data in an electronic format.

1.4.3. **Administrative information** is any data related to the business of AC including, but not limited to, financial, personnel, student, alumni, and physical resources. It includes data maintained for the purposes of AC business regardless of the media or location. Administrative information does not include library holdings or

instructional notes unless they contain information that relates to a business function.

1.4.4. **Confidential information** requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of AC to accomplish its mission as well as records about individuals requiring protection under the Family Educational Rights and Privacy Act (FERPA). Confidential information includes, for example, student financial aid information, alumni gifts and student grades.

1.4.5. **Sensitive information** requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to AC. It is assumed that all output is classified as sensitive unless otherwise indicated. Sensitive information includes, for example, class lists, contract data, and vendor data information.

1.4.6. **Public Information** can be made generally available both within and beyond AC. It should be understood that any information that is disseminated within the campus community is potentially available to the public at large in accordance with the Texas Public Information Act and the United States Freedom of Information Act (FOIA). Public information includes, for example, telephone directory information.

1.4.7. **Student Directory Information** is information available for public consumption unless the student specifically directs that it be withheld. The student may direct the Office of the Registrar not to disclose such information. Public directory information as defined by FERPA includes:

a) student's name
b) participation in officially recognized activities
c) address
d) telephone listing
e) electronic mail address
f) photograph
g) degrees, honors, and awards received
h) date and place of birth
i) major field of study
j) dates of attendance
k) the most recent educational agency or institution attended

1.4.8. **Network devices** will include but not be limited to hubs, switches, routers, wireless access points (WAPs), networked printers, and wireless printers.

1.5. Ownership of Electronic Files

1.5.1. Electronic files created, sent, received, or stored on the AC ITS resources are the property of AC with custodial/ownership responsibilities designated by the appropriate executive-level administrator designated by the President. Custodians of record and/or owners of electronic information will work with the Chief Information Officer & Dean of Information Technology Services (CIO) to ensure compliance with Texas Administrative Code 202, which includes business functional information in the following categories:

a) social security numbers
b) credit card information
c) other personal financial information
d) student records
e) health information
f) restricted personal information – includes other data protected under state or federal law
g) mission critical information – includes information vital to AC operations
h) non-critical information – includes information that is generally available to the public or has minimum impact on AC operations

1.6. Policy Statements

1.6.1. Access to data is authorized by the custodian of record and/or owner of electronic information. Access is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. Access cannot be shared, transferred or delegated. (see 1.7.1)

1.6.2. AC recognizes administrative information as an AC resource requiring proper management in order to permit effective planning and decision-making and to conduct business in a timely and effective manner. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment.

1.6.3. AC retains ownership of all administrative information created or modified by its employees as part of their job functions.

1.6.4. Access to the network, data, and administrative information will be restricted by login ID's and passwords.

1.6.4.1. Passwords must be changed by the user every sixty days. See procedure 1.7.4.

1.6.4.2. Passwords must not be shared.

1.6.4.3. Passwords must not be written down or otherwise recorded in ways that they may be easily found by an unauthorized person.

1.6.4.4. Individuals are expected to protect passwords from disclosure.

1.6.5. Data and administrative information will be used for its designed college business purpose only.

1.6.6. Data and administrative information will not be shared with external entities without supervisor or manager approval. See procedure 1.7.5.

1.6.7. ITS personnel will adhere to guidelines set forth in the Privileged Access Agreement.

1.6.8. Users will assure data integrity by contacting both supervisors and appropriate ITS personnel immediately if data is suspected of corruption or inappropriate changes.

1.6.9. It is the user's responsibility to protect access to data (e.g., screensaver passwords, logging off, securing paper documents, etc.) under their control.

1.6.10. Users may not disclose data to others, except as required by their job responsibilities.

1.6.11. Users may not use AC data for their own personal gain, nor for the gain or profit of others.

1.6.12. Users may not access data to satisfy their personal curiosity.

1.6.13. Employee information may include some or all of the following: name, department, position title, campus address, campus phone and email address. These data are available on-line from AC homepage. Employees may request that personal data be classified as confidential. All other employee related data, especially that which is available to users outside Human Resources (HR) such as social security number and birth date, must be vigilantly safeguarded and treated as confidential.

1.6.14. Employees are responsible for safeguarding student information as defined in section 1.4.7.

1.6.15. HR will notify ITS immediately upon termination or change in an employee's position to disable or change account access for that employee. (see 1.7.2)

1.7. Guidelines and Standard Operating Procedures (SOP)

1.7.1. Supervisors of new employees to the department/division must complete the Employee Access Request Form. ITS will notify supervisors when access has been set up.

1.7.1.1. It is the supervisor's responsibility to explain the access policies, rights, and responsibilities.

1.7.2. Network Devices

1.7.2.1. It is the position of Amarillo College that all network devices not originating from Network Services or the ITS Division be listed with said areas within five business days. Any device discovered, whether through physical or electronic means will be considered a rogue device and appropriate corrective action taken. The devices will be allowed after they are registered and verified compliant with the proper security policies of Network Services. Registration of devices will include at minimum device type, make and model, department that it will be used in, location within the department and the name of a person in the department that will be responsible for the device.

1.7.3. Modification and Termination

1.7.3.1. HR and supervisors will report new hires, transfers and terminations to the ITS Helpdesk. A work order will be generated to the ITS System Administrator to disable/modify all account access for that employee.

1.7.3.2. A security access program will be run by ITS staff monthly to determine if individuals are no longer employed and access needs to be removed or if individuals have changed job roles which may need to have access rights reviewed/modified.

1.7.3.3. ITS System Administrators will review reports identifying failed login attempts, including unsuccessful attempts by individuals to access portions of the system to which they are not authorized. After five consecutive failed login attempts, accounts are automatically deactivated. ITS will immediately notify the Department security manager and other appropriate AC officials if it appears security has been breached.

1.7.4. Passwords

1.7.4.1. ITS will configure the system so that passwords will expire after sixty days and prompt the user to change.

1.7.5. Release of Data and Administrative Information to External Entities

1.7.5.1. Requests for release of administrative information are referred to the office responsible for maintaining those data.

1.8. Disciplinary Actions

Violation may result in a denial of access to AC computer resources, and those disciplinary actions provided or authorized by the rules and regulations of AC through the Office of Human Resources or Student Services.

1.9. Reference Information

Gramm-Leach-Bliley Act of 2000 (GLB)
www.ftc.gov/privacy/glbact/glbsub1.htm

Federal Trade Commission (FTC)

Family Educational Rights and Privacy Act (FERPA)
www.ed.gov/policy/gen/guid/fpco/**ferpa**/index.html

Texas Public Information Act (Texas Open Records Act)
http://www.oag.state.tx.us/AG_Publications/pdfs/publicinfo_hb2008.pdf

United States Freedom of Information Act

http://www.usdoj.gov/oip/foiastat.htm, http://www.usdoj.gov/oip/amended-foia-redlined.pdf