# Policy for the Responsible Use of Information and Technology Resources

**Responsible Department:** Information Technology
**Responsible Administrator:** Kay Reeves, Executive Director for Information Technology
**Effective Date:** August 1, 2010
**Reviewed/Updated Date:** August 1, 2013
**Date of Scheduled Review:** August 1, 2015

## I. PURPOSE

This policy is designed to perpetuate ACU's academic, research, and service mission by defining the appropriate and responsible use of the information and technology resources at ACU. Each authorized user of these resources must assume responsibility for his/her own behavior while utilizing these assets. Users of these resources should accept that the same morality and ethical behavior that serve as guides in its non-technology environments should also serve as guides in its information and technology environment. It is imperative that the campus community understands that information and technology resources require responsible behavior from all its users.

## II. SCOPE

This policy applies to all faculty, staff, students, contractors or any other individual using information and technology at ACU. Access to ACU-owned hardware, software and support provided by technology staff members is a privilege and not a right. Accepting access to this information and technology carries an associated expectation of responsible and acceptable use. When accessing any remote resources using ACU technology resources, users are required to comply with both the policies set forth in this document and all applicable policies governing the use and access of the remote systems. When these policies conflict with each other, this policy and all other ACU policies will supersede the remote system's policies.

## III. DEFINITIONS

Computer - An electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses, and that includes all input, output, processing, storage, software, and communication facilities that are connected or related to an electronic system or communication network.

Computer hardware - Any and all tangible or physical devices attached to or used in conjunction with a computer system.

Computer network - The interconnection of communication lines, including wireless connections, with a computer through remote terminals or a complex consisting of two or more interconnected computers.

Computer program - An ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

Computer resources - Any and all computerized institutional data, computer hardware, and computer software owned by or operated at ACU.

Computer software - A set of computer programs, procedures, or associated documentation used in the operation of a computer system.

Computer supplies - magnetic tape, tape cartridges, diskettes, floppy diskettes, compact discs, and computer output, including paper, magnetic, optical, or other media.

Computer system - A set of related computer equipment, hardware or software.

Data - A representation of information, knowledge, facts, concepts, or instructions that have been prepared or are being prepared in a formalized manner and have been processed, are being processed, or are intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, compact discs, and as stored in the memory of ACU computers. Data are property.

Data Steward - Individual responsible for the accuracy and institutional responsibility for a set of data, e.g., Human Resources Director for personnel and payroll data, Registrar for student records.

Institutional policy - A succinct and cogent written document bearing the approval of the President's Cabinet of the university that clearly defines faculty, staff, student, and institutional responsibilities within a prescribed area of campus existence.

Property - Anything of value, including but not limited to financial instruments, information, electronically produced data, computer software, and computer programs.

Responsible use - Any action or behavior of an individual that does not cause accidental or unauthorized destruction, disclosure, misuse, or modification of or access to the information technology or computer resources owned or operated by ACU.

Technology resources - Any and all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data.

User - Any person authorized to access and use the information technology resources at
ACU.

User account - Any logical access on any ACU computer system that has been specifically established for a particular user. A user account may have a dedicated logical area on one or more ACU computer system also associated with it.

## IV. PROCEDURE (OR PROCESS)

SECTION ONE – GENERAL

1.1 Access & Privileges

1.1.1 User Accounts

ACU faculty, staff, students, contractors or any other individual using information and technology at ACU are provided access as outlined in ACU's Account Management Policy to various information systems and technology based upon their individual role and need. These accounts may include, but are not limited to: individual computers or workstations accounts, personal network file-space accounts, directory services accounts (i.e. AD, LDAP and SSO), applications accounts (i.e. email, ERP, LMS, CMS, CRM, etc.) and others. Access to these accounts is a privilege not a right and may be revoked for any reason including non-compliance with ACU's Account Management Policy.

1.1.2 ACU ID

Users are responsible for all activity performed with their ACU ID. ACU IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their ACU IDs. Similarly, users are forbidden from performing any activity with ACU IDs belonging to other users. Any suspected unauthorized access of a user account should be reported immediately to the Chief Information Officer, the Executive Director of Information Technology or their designee.

1.1.3 Passwords

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms, so long as doing so does not violate any policies, regulations or practices related to PII, FERPA or HIPPA. All users are responsible for both the protection of their user account password and the data stored in their user account.

### 1.1.4 System Privilege Deactivation

All accounts may be deactivated if account privileges are no longer commensurate with an individual's function at the university or their need to know due to a change in their status. See employee specific and student specific deactivation policies in the Account Management Policy.

### 1.1.5 No Responsibility for Personally Owned Computers

ACU cannot provide, and will not be responsible for, software or data kept on personally owned computers, nor is it responsible for the installation, repair, maintenance or upgrade of personally owned hardware.

## 1.2 Acceptable Use

### 1.2.1 Acceptable Uses of Information and Technology Resources

All information and technology resources at ACU are provided to assist faculty, staff, students, contractors or any other individual in acquiring and disseminating information related to the performance of regularly assigned job duties, classroom assignments, or scholarly research.

### 1.2.2 Unacceptable Uses of Information and Technology Resources

Any information, data, or programs not congruent with the mission of ACU must not be created, stored, transmitted, viewed or manipulated using ACU-owned technology or information systems.

The following is a list that includes, but is not limited to unacceptable uses of information and technology resources at ACU.

A) Transmitting any material, or engaging in any other activity in violation of any federal, state, or local laws, including U.S. and international copyright law or trade agreements.

B) Transmitting or accessing information containing harassing material. Electronic harassment includes, but is not limited to:

i. Text images with the intent to harass, terrify, intimidate, threaten or offend another person

ii. Contact of another person with the intent to harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease

iii. The disruption or damage of academic, research, administrative or related pursuits of another

iv. Invading the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

C) Transmitting, receiving, displaying, or viewing offensive content, which includes, but is not limited to:

i. sexual comments or images

ii. racial slurs

iii. gender specific comments or any comments that would offend someone on the basis of their age, sex, national origin or disability

iv. Displaying, sending, printing, or storing sexually explicit, graphically disturbing, obscene, pornographic, fraudulent, harassing, threatening,

abusive, racist, or discriminatory images, files or messages in any campus computing facility or any campus location.

D) Disseminating or printing copyrighted materials, including computer files, articles and software, in violation of U.S. and international copyright laws or trade agreements

E) Attempting forgery of email messages

F) Physical or electronic interference with other computer systems users

G) Any other practice or user activity that, in the opinion of management constitutes irresponsible behavior, promotes illegal activities, results in the misuse of resources or jeopardizes the operation of information and technology resources at ACU.

### 1.2.3 Prohibition Against Commercial Use of Information Resources

ACU users must not use ACU information and technology resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by ACU administrators. Prohibited activity includes, but is not limited to operating a business, usurping business opportunities or soliciting money for personal gain.

## 1.3 Privacy and Data Ownership

### 1.3.1 Legal Ownership of Information Systems Files and Messages

ACU has legal ownership of the contents of all files stored on its information and technology resources as well as all content transmitted via these systems. ACU reserves the right to access all such information without prior notice whenever there is a genuine business need.

### 1.3.2 No Responsibility for Monitoring Content of Information Systems

ACU reserves the right to remove any message, file, database, graphic, or other material from its information and technology resources. At the same time, ACU has no obligation to monitor the information content residing on or flowing through those systems.

### 1.3.3 Privacy Expectations and Information Stored on ACU Systems

At any time and without prior notice, ACU reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on ACU information and technology resources. Similarly, at any time and without prior notice, ACU reserves the right to examine or monitor any device attached, for any reason, to the ACU network. This examination is performed to ensure compliance with internal policies, to support the performance of internal investigations, to comply with legal requirements such as a subpoena or court order, and to assist with the management of ACU's systems. It is also possible that other individuals, organizations and agencies, with permission from ACU administrators, may likewise access or monitor these same systems, whenever there is a legitimate business need of ACU for them to do so.

### 1.3.4 Disclaimer of Responsibility for Damage to Data and Programs

ACU uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by information and technology resources. In keeping with these objectives, ACU maintains the authority to:

a. restrict or revoke any user's privileges,

b. inspect, copy, remove, or otherwise alter any data, program, or other resource that may undermine these objectives, and

c. take any other steps deemed necessary to manage and protect those systems. This authority may be exercised with or without notice to the involved users. ACU disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

## 1.4 Intellectual Property

### 1.4.1 - Copyright Laws

Unless placed in public domain by its owners, Section 117 of the 1976 Copyright Act protects software programs. Software is also protected by the license agreement between the owner and purchaser. It is illegal to duplicate, copy, or distribute software or its documentation without the permission of the copyright owner.

### 1.4.2 - Software

Respect for the intellectual work and property of others has traditionally been essential to the mission of academic institutions. As members of the academic community, ACU values the free exchange of ideas. Just as ACU does not tolerate plagiarism, ACU strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet users or other system users make unauthorized copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by ACU.

### 1.4.3 Fair use

Unless permission from the copyright owner(s) is first obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

## SECTION TWO – SPECIFIC POLICIES FOR STUDENTS

### 2.1 Student Specific Privileges

#### 2.1.1 System Privilege Activation

ACU information and technology resources privileges are activated at the time that a student is admitted to ACU. The specific time an account is active may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. All normal access, defined as access necessary for an individual to perform the tasks expected of their role at the university, and only normal accesses, are created when the student is admitted to the university and will persist so long as the individual remains an active participant in the ACU community. More specific references can be found in the Account Management Policy.

#### 2.1.2 System Privilege Deactivation

All ACU information and technology resources privileges are deactivated at the time that a student is no longer an active member of the ACU community. The time frame for deactivation may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. All data, files, or messages may be removed from user accounts when account deactivation occurs. More specific references can be found in the Account Management Policy.

### 2.2 Campus Computing Facilities

#### 2.2.1 Acceptable Use of Facilities

Computer labs on the ACU campus are not available for general use during the periods when the rooms have been reserved for teaching purposes, unless otherwise specified by the professor. Facilities are often made available on an unmonitored basis. It is the responsibility of every user to use these facilities in a responsible manner.

#### 2.2.2 Disruptive Behavior

Students using campus computing facilities must not cause unnecessary noise, display abusive or inappropriate behavior towards other users, or create other disturbances in any campus computing area.

#### 2.2.3 Data Protection

Students using campus computing facilities must not access, destroy or remove data other than their own.

#### 2.2.4 Destruction of Computer Resources

Students using campus computing facilities must not destroy or remove university owned computer resources.

#### 2.2.5 Alteration of Lab Computer Set-Up

Students using campus computing facilities must not attempt to change the hardware and software configurations on ACU-owned computers.

### 2.2.6 Damage Reporting

Students using campus computing facilities must report accidental damage or damage caused by other parties to the Team55.

## SECTION THREE – SPECIFIC POLICIES FOR EMPLOYEES (Faculty, Staff and Student Employees)

### 3.1 Privileges

#### 3.1.1 System Privilege Activation

ACU information and technology resources privileges are activated at the time that an individual is hired as an employee of ACU. The specific time an account is active may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. All normal access, defined as accesses necessary for an individual to perform the tasks expected of their role at the university, and only normal accesses, are created at the point of hire and will persist so long as the individual remains an active participant in the ACU community. More specific references can be found in the Account Management Policy.

#### 3.1.2 System Privilege Deactivation

All ACU information and technology systems privileges are deactivated at the time that an employee ceases to provide services to ACU. The time frame for deactivation may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. (See Exception to System Privileges). All data, files, or messages may be removed from user accounts when account deactivation occurs. More specific references can be found in the Account Management Policy.

#### 3.1.3 Exception to System Privilege Deactivation

ACU retirees are eligible to receive access to an ACU email account using their ACU ID and password. This is a privilege and may be revoked at any time. Retirees must agree to abide by all ACU information policy in order to maintain their account.

#### 3.1.4 Incidental Personal Use of Information Resources

ACU allows computer users to make reasonable and incidental personal use of ACU's information and technology resources. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, and (c) does not preempt any business activity. All such personal use must be consistent with conventional standards of ethical and polite conduct. For example, electronic mail must not be used to distribute or display messages or graphics that may reasonably be considered by some to be disruptive or offensive (such as sexual jokes or pornography).

### 3.2 Privacy

#### 3.2.1 Privacy / Administrative Data

Security and confidentiality are matters of concern to all ACU employees who have access to information and technology resources. ACU is responsible for the accuracy, integrity and confidentiality of its electronic databases. All administrative electronic data must be treated as confidential, other than data that has been designated as approved for

release to the public by ACU administrators. By law, certain electronic institutional data are confidential and may not be released without proper authorization. Since conduct, either on or off the job, could affect or threaten the security and confidentiality of this information, each employee who accesses any ACU information and technology resource is required to adhere to the following:

3.2.1.1 No one shall make or permit unauthorized use of any information in files maintained, stored, or processed by any ACU software.

3.2.1.2 No one is permitted to seek personal benefit, allow others to benefit personally or to divulge, in any way, the contents of any record or report, to any person except in the conduct of his/her work assignment.

3.2.1.3 No one shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry. No one shall knowingly change or delete or cause to be changed or deleted an entry in any record or report, unless expressly authorized to do so and in accordance with approved policies and procedures.

3.2.1.4 Once information is downloaded, data should not be altered in word processing documents or spreadsheets in a way that misrepresents the information derived from these data. Downloaded information should be used and represented responsibly.

3.2.1.5 No official record or report, or copy thereof, shall be removed from the office where it is maintained or copied or printed via electronic means except in the authorized performance of a person's duties, and in accordance with established procedures. Copies made in the performance of a person's duties shall not be released to third parties except as in paragraph 3.2.1 above applies.

3.2.1.6 No one is to aid, abet, or act in conspiracy with another to violate any part of these terms and conditions.

3.2.1.7 Any knowledge of a violation of these terms and conditions must immediately be reported to the employee's supervisor and the Chief Information Officer, the Executive Director of Information Technology or their designee.

3.2.1.8 Computing devices shall not remain logged on to ACU's campus network when unattended, unless they are logically locked down by a standard operating system lock feature.

## 3.3 When Making Copies of Software is Permissible

Third party software in the possession of ACU must not be copied unless such copying is consistent with relevant license agreements and either: (a) management has previously approved of such copying, or (b) copies are being made for contingency planning purposes.

## 3.4 Data Steward

Data Stewards are designated individuals who have the ultimate responsibility for the accuracy and completeness of data in their respective areas. Examples include the Registrar for student data and the Director of Human Resources for employee data.

### 3.4.1 User Profile Groups

Data Stewards are responsible for maintaining security group assignments (user profiles that represent what is needed to perform a general set of related tasks.)

### 3.4.2 Access to Data

The appropriate Data Steward must approve all access to institutional data. By approving access, the Data Steward consents to the use of these data within the normal business functions of administrative and academic offices.

Access to institutional data shall not be granted to persons unless there is documented businesses need to know.

### 3.4.3 Violation of Access Privileges

The Data Steward reserves the right to determine appropriate use of the data under his/her control. Usage violations may result in revocation of a user's access to the data.

## SECTION FOUR – SPECIFIC POLICIES FOR INFORMATION PROFESSIONALS

### 4.1 Handling of Third Party Confidential and Proprietary Information

Unless specified otherwise by contract, all confidential or proprietary information, including software written by a third party, that has been entrusted to ACU by a third party must be protected as though it was ACU confidential information.

### 4.2 Confidentiality of ACU Computer Related Software or Documentation

All ACU generated programs, codes and related documentation is confidential and must not be taken elsewhere when an employee, consultant, or contractor leaves the employ of ACU.

### 4.3. Removal of Sensitive Information From ACU Premises

Confidential ACU information, no matter what form it happens to take, must not be shared with those outside of ACU, or removed from ACU premises, unless there has been prior approval from the Data Steward.

### 4.4 Copyright Notices on Computer Programs and Documentation

All computer programs and program documentation owned by ACU must include appropriate copyright notices.

## SECTION FIVE – META POLICY

### 5.1. Policy Revision and Review

#### 5.1.1 Additions and Deletions

Suggested information policy additions, deletions or alterations must be submitted to the Chief Information Officer, the Executive Director of Information Technology or their designee, in order to be implemented

#### 5.1.2 Policy Review Committee

A policy review committee will be comprised of the Chief Information Officer, the Executive Director of Information Technology, the Executive Vice President, the Provost, the Director of Human Resources and the University Counsel. Any member of this committee may request additional review by others, but policy acceptance will occur when each of the members comprising this committee have signed in approval. Policy specifically designated for Information Professionals, will be at the approved by the Chief Information Officer, the Executive Directory of Information Technology and the Executive Vice President.

#### 5.1.3 Policy File

A file will be kept by the Chief Information Officer maintaining this policy and the approval documents for this policy for at least ten years.

#### 5.1.4 Policy Communication

ACU Information Policy will be available on a web site

#### 5.1.5 Policy Summaries

Condensed versions of this policy or user-specific synopses of these policies may be distributed as needed to adequately implement the policies. Condensed versions or synopses must include information about how to obtain the complete policy or policies.

## V. COMPLIANCE (Optional)

All users of ACU information and technology resources are required to comply with this policy. ACU reserves the right to deny, to limit, to restrict or extend privileges and access to its information and technology resources.

## VII. MISCELLANEOUS (Optional)

ACU, through an appropriate review and amendment process, reserves the right to amend this policy at any time and without prior notice in order to provide better information and technology access to faculty, staff, students, contractors or any other individual using these resources at ACU.