Amended 1/18/05 by CCE Executive Committee

CULLEN COLLEGE OF ENGINEERING POLICIES AND PROCEDURES FOR DEPARTMENTAL COMPUTING

PURPOSE Procedures for departmental computing are designed to provide accountability for computer usage in accordance with accepted standards of internal controls.

REFERENCES SAM 07.A.02, SAM 07.A.03, SAM 07.A.04, MAPP 10.03.01, MAPP 10.03.02, MAPP 10.03.03, MAPP 10.03.04, IT Reference Guide, IT Support Center Standards

I. General Statement

Procedures for departmental computing are designed to provide accountability for computer usage in accordance with accepted standards of internal controls. All employees of the Cullen College of Engineering (CCE) are responsible for complying with the policies and procedures described below. Failure to adhere to these policies and procedures may result in disciplinary action being taken against the employee. Compliance with these procedures will help protect employees when questions arise and protect the University from criticism by auditors and other reviewing officials.

All employees have an obligation to report any suspected misuse, abuse, or security violations related to computer use. Employees who are aware of criminal activity and fail to report such may be subject to disciplinary action. Employees are required to cooperate with any police or audit investigation, and they may be requested to keep their knowledge of the investigation confidential.

The policies set forth within this document are CCE policies and speak to all departments and units under the jurisdiction of the Dean of Engineering.

II. Guidelines

SAM 07.A.02
SAM 07.A.03
SAM 07.A.04

MAPP 10.03.01
MAPP 10.03.02
MAPP 10.03.03
MAPP 10.03.04

IT Reference Guide
IT Support Center Standards

III. Responsible Parties within CCE

Dean of Engineering/Department Chairs/Program Directors: responsible for ensuring that all faculty and staff within their "unit" are cognizant of and subsequently adhere to CCE Policies and Procedures for Departmental Computing.

Associate Dean of Research/Department Chairs: responsible for ensuring that all faculty within the CCE are cognizant of and subsequently adhere to CCE Policies and Procedures for Departmental Computing regarding backing up research data relevant to their scholarship (publications, grants, and contracts

College of Engineering Business Administrator: responsible for maintaining and backing up relevant financial information for operation within the Dean's office and supporting units that report through the Dean's office.

Department and Program Level Business Administrators: responsible for maintaining and backing up relevant financial information for operation within their Department/Program and supporting units that report through the Department/Program.

Director, Information Systems and Services: responsible for providing and maintaining appropriate hardware and software in order for the responsible parties in the College to adhere to CCE Policies and Procedures for Departmental Computing.

IV. Policy Provisions

The Cullen College of Engineering will provide disk storage space for all departments and units to abide by CCE Policies and Procedures for Departmental Computing relevant to the back up of financial data.

All departments and units MUST use the disk storage space provided by the CCE to comply with CCE Policies and Procedures for Departmental Computing relevant to the back up of financial data effective March 1, 2005 unless written authorization is granted by the Dean of Engineering.

All departments and research units must submit to the Dean of Engineering annually (March 1 of each year) for approval their plan to ensure that CCE Policies and Procedures for Departmental Computing regarding the back up of research data.

All computer systems requiring log-on and password shall have an initial screen banner reinforcing security requirements and reminding users of their need to use computing resources responsibly.

Each computer account will be assigned to a single individual who is accountable for the activity on that account.

Users shall not seek or reveal information on, obtain copies of, or modify files, tapes, or passwords belonging to other users, nor may the user misrepresent others.

Users must abide by the laws protecting intellectual property, copyright and licensing of programs and data. In no case will copies be made of a licensed computer program to avoid paying additional license fees or to share with other users.

System Administrators and other custodians of computers are responsible for the security of university hardware, software, networks and data entrusted to their use. This security includes the following provisions:

Ensuring doors to areas with computer equipment are locked and/or that computer security devices to secure computers to desks are installed;

Ensuring that computer equipment is protected from weather, chalk dust, and other foreign materials;

Securing floppy disks and floppy drives;

Backing up all critical data files and storing back-up data in a secure, separate area;

Ensuring that data storage/disk space on computers is adequate for departmental usage;

Ensuring that the latest version of anti-virus software is installed on computers and is being used;

Use of surge protectors or uninterrupted power supply (UPS) to protect equipment and data in case of electrical power failure;

Responsible for taking all possible precautions to protect the security of programs and operating systems under their care against network intrusions and other unauthorized access.

V. Password Control

Computer accounts are to be assigned to the individual employee or issued on an individual employee basis if computerized records are being accessed as part of their responsibility.

Passwords will be a minimum length of five characters and if stored on the computer needs to be encrypted in storage.

Passwords which are obvious, such as words (English or otherwise), nicknames, dates of birth, phone numbers, social security number, etc., should not be used. Never use an all-numeric password. Do use a mixture of alphabetic (upper & lower case) and numeric characters.

Passwords should be changed on a regular basis, never shared with others, and not written down.

VI. Risk Assessment Policy

The Director for Information Systems Services for the CCE in consultation with CCE Department Chairs, the CCE Associate Dean for Research, and Program Directors will annually conduct a risk assessment program consisting of the following:

Identification of assets
Estimation of asset values
Identification of threats
Identification of vulnerabilities
Calculation of risk

The Risk Assessment policy will be submitted annually (March 1 of each year) to the Dean of Engineering for review. The report will update significant changes which have occurred over the previous 12 month period.