SECTION: Information Technology **Number: 10.03.06**
AREA: User Responsibilities

SUBJECT: College/Division Responsibilities for Information Technology Resources

I. PURPOSE AND SCOPE

This document delineates responsibilities of the colleges and divisions for the management of information technology resources under their purview. Business and academic processes are increasingly dependent on computers and computer-based information systems. The application of an increasing number of federal and state laws, industry standards and contractual obligations require management oversight and uniform policies for the governance of information technology resources. Given this environment, roles and responsibilities for managing departmental information systems will be developed at the unit level to ensure controls, the safeguarding of departmental information technology resources, and compliance with related university policies.

II. POLICY STATEMENT

A. The management of each college, division and unit is responsible for the administration and protection of its information technology resources, and for ensuring compliance with this and other university information technology policies. College and division management will develop departmental policies and procedures, and establish internal controls to address the use of information technology resources in the following areas:

1. Risk Management: Assess departmental functions and activities at risk; develop strategies and implement plans to mitigate risk, including the protection of data, and incident handling and priority notification procedures; justify and document areas where unit management has chosen not to implement comprehensive risk mitigation measures (acceptance of risk).

2. Resource Security: Develop appropriate administrative, technical and physical security controls over information resources; ensure proper information back-up and record retention procedures.

3. Service Continuity Management: Develop and implement plans to ensure the timely restoration of essential departmental information technology functions (administrative, research, instruction, etc.) and information in the event of a disaster or significant interruption of normal business activities.

4. Resource Management: Plan for lifecycle management – acquisition, maintenance, and disposal – of information resources (hardware and software).

B. Each college and division will assign the following roles for the management of information technology resources:

1. College/Division Information Resource Manager (C/D-IRM): The most senior administrator who is responsible for managing and securing the college or division's Information Resources, including the related planning and compliance processes. This role is often filled by a college's Assistant/Associate Dean or a division's Assistant/Associate Vice President.

2. College/Division Technology Manager (C/D-TM): An IT professional who is responsible for managing the college or division's daily Information Technology operations. This role is often filled by a Director or Manager.

3. College/Division Information Security Officer (C/D-ISO): The employee responsible for managing the college or division's information security function in accordance with the established policies and guidelines. This role is often filled by a Director or Manager.

C. In addition to on-going services to individual students, faculty and staff, and oversight of enterprise-level software and systems, the University of Houston Information Technology (IT) Department will provide to college/division information technology providers consultative, best practice services for the areas described in Section II.A, including:

1. Facilitate university-wide coordination of and planning related to the information technology areas described in Section II.A.

2. Training to college/division-based technical support staff.

3. Technical guidelines and reference materials.

4. Coordination of meetings of the C/D-IRMs, C/D-TMs, C/D-ISOs, and relevant subject-matter experts.

5. As-needed facilitation of college-based IT initiatives.

The IT Support Center will be the central point of contact for these services.

D. The University of Houston will safeguard its information assets in all areas of operation. Therefore, each unit will adhere to applicable requirements of:

1. Gramm-Leach-Bliley Act (GLBA): Requirement of institutions engaged in financial transactions to protect the security and confidentiality of customers' nonpublic personal information.

2. Family Educational Rights and Privacy Act (FERPA): Protects the privacy of student education records.

3. Health Insurance Portability and Accountability Act (HIPAA): Health information privacy and security standards.

4. Texas Administrative Code: Information Security Standards (1 TAC 202) - Texas state regulations for the protection of the information assets of state agencies and universities.

5. Payment Card Industry (PCI) Data Security Standard: Credit card company's information security standard for the protection of cardholders' data required of all merchants and entities accepting credit cards or processing credit card transactions.

6. Other applicable statutory requirements, contractual obligations and industry standards regarding the protection of information and information assets.

III. DEFINITIONS

Definitions of terms used in this policy may be found in the Glossary of Information Technology Terms, 10.00.00.

IV. GENERAL PROVISIONS

A. The University of Houston Information Technology Department (IT) will provide materials, consultation, and training to facilitate departmental compliance with this MAPP. See Section V.II. for references and links.

B. Colleges and divisions will review their procedures annually and update them as appropriate.

V. REVIEW AND RESPONSIBILITIES:

Responsible Party: Associate Vice President for Information Technology and Chief Information Officer

Review: Every 3 years, on or before June 1

VI. APPROVAL

Jim McShan
Interim Vice President for Administration and Finance

Donald J. Foss
Senior Vice President for Academic Affairs and Provost

Renu Khator
President

Date of President's Approval: April 7, 2008

VII. REFERENCES

System Administrative Memorandum 07.A.02 – The Ethical and Legal Use of Micro/Personal Computer Software
System Administrative Memorandum 07.A.03 – Notification of Automated System Guidelines
System Records Retention Schedule
Manual of Administrative Policies and Procedures 10.03.01 – Computer User Responsibilities
Manual of Administrative Policies and Procedures 10.03.02 – Computer and Network Security
Manual of Administrative Policies and Procedures 10.03.03 – Security Violations Reporting
Manual of Administrative Policies and Procedures 10.03.04 – Connecting Devices to University Networks
UH Information Security Manual
UH IT General Computing Policies
UH IT Reference Guide
UH IT Support Center Standards
Federal Computer Security Act of 1987
Texas Penal Code Chapter 33
Gramm-Leach-Bliley Act, Section 15 USCA 6801 et al., Section 16 CFR 314 et al.
Family Educational Rights and Privacy Act
Health Insurance Portability and Accountability Act
Texas Administrative Code: Information Security Standards (1 TAC 202)
Payment Card Industry (PCI) Data Security Standard

Index terms:
Business continuity planning
Computer and computer-based information systems
Computer user responsibilities
Data back-up and record retention
Disaster recovery
Information technology assets
Management of information technology resources
Misuse of computer equipment and systems
Risk management
Safeguarding departmental information technology resources
Security
Security access controls