UNIVERSITY of HOUSTON
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

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

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, and the Texas Administrative Codes applicable to institutions of higher education, which are administered by the Texas Department of Information Resources (http://www.sos.state.tx.us/tac/index.shtml). 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).

5.　Project Management: Plan and manage projects using practices with appropriate levels of integration, scope, schedule, cost, quality, resources, communications, risk, and procurement management.

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, acquiring and/or developing, and securing the college or division's information resources, including related information technology planning, technology project and portfolio management, and compliance processes. This role is often filled by a college's assistant/associate dean or a division's assistant/associate vice president. For the scope of their job that involves management of information resources, they shall have a dotted reporting line to the university's chief information officer. The C/D-IRM is responsible for ensuring an Information Resource Management Plan is created and maintained for their area.

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 and projects, including the definition of IT opportunities and needs for review/approval by the C/D-IRM, and the execution of approved projects in accordance with established policies and standards. This role is often filled by a director or manager and should report to the C/D-IRM.

3.   College/Division Information Security Officer (C/D-ISO): The employee responsible for managing the college or division's information security functions in accordance with the established policies and guidelines. This role is often filled by a director or manager and should report to the C/D-IRM or directly to the vice president of the division or dean of the college.

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

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

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

3.   Templates, 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.

D.   The university 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.   Texas Administrative Code: Project Management Practices (1 TAC 216): Texas state regulations for the management of IT projects conducted by state agencies and universities.

6.   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.

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

III.   GENERAL PROVISIONS

A.   UIT will provide materials and training to facilitate departmental compliance with this policy. UIT is available for consultation upon request.

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

IV.   REVIEW AND RESPONSIBILITY:

Responsible Party: Associate Vice President for Information Technology and CIO

Review: Every three years on or before June 1

V.   APPROVAL

_____Jim McShan_____
Senior Vice President for Administration and Finance

_____Renu Khator_____
President

Date of President's Approval: _____June 4, 2018_____

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	04/07/2008	Initial edition
2	03/03/2011	Updated MAPP template to reflect current operating requirements. Added links to documentation as applicable. Updated Section II.A, adding Project Management as Section II.A.5 and Section II.B to reflect current operating requirements. Changed IT Support Center to Technology Partners Program throughout. Added Section II.D.5 on 1 TAC 216. Removed Section III, Definitions. Removed the Chief Information Officer as a Responsible Party. Added Executive Vice President for Administration and Finance to approval cycle. Added references to Section VI. Removed Index Terms
3	12/11/2015	Added new Revision Log. Added the responsibility for creating and maintaining an Information Resource Management Plan for the College/Division Information Resource Manager to Section II.B.1. Removed Technology Partners Program as central point of contact for best practices services in Section II.C. Added University Information Technology (UIT) throughout procedure as applicable. Removed Section VI, References
4	06/04/2018	Minor housekeeping changes only to Sections II.B.2 and II.B.3. No additional changes were made by the Subject Matter Experts (SMEs)