Policy IT-PO2

Administrative Office Roles and Responsibilities for Information Resources

Contents

I.   **Title**

Administrative Office Roles and Responsibilities for Information Resources

II.   **Policy**

This policy establishes roles and responsibilities for coordinating information resources at The University of Texas at Arlington.

This Policy does not replace or supersede, but rather is intended to complement (and should be interpreted consistently with) Federal, State, University of Texas System and UT Arlington regulations, policies, standards and procedures that deal with the use of Information Technology ("IT") and information security, and is drawn from State of Texas Administrative Code 202, University of Texas System Policy 165 and other relevant UT Arlington policies.

A.   **Responsibilities**

1.   **Risk Management:** Coordinate and/or perform regular review of risks related to information resources, plan and execute mitigation strategies, develop procedures for prioritizing and handling incidents, and document appropriate justification for not undertaking mitigation measures where the office has chosen to accept a risk related to information security.

2.   **Resource Security:** Coordinate and/or perform the development and implementation of procedures, practices, and technology to safeguard information resources consistent with the UT System Information Security Program Elements and those established by the Information

Security Office.

3. **Compliance:** Ensure that information resources are properly protected through the coordination and/or development of internal procedures and practices which maintain compliance with all applicable federal, state, and local laws including, but not limited to, the relevant policies listed in Sections IV and V.

4. **Service Continuity:** Coordinate and/or develop plans and procedures for ensuring operational continuity of information technology required for performing critical business functions as outlined in *Business Continuity Policy* ([Policy 5-306](#)).

5. **Resource Management:** Coordinate and/or develop plans and procedures for acquiring, maintaining, and disposing of information resources (hardware, software, and data) in accordance with relevant policies and procedures (including, but not limited to, those listed in Sections IV and V), contractual obligations, and/or vendor or University support life cycles.

6. **Project Management:** Manage or ensure the management of IT projects through a methodology that adequately manages technology integration, scope, schedule, cost, quality, resources, communication, risk(s), and procurement as outlined in [Texas Administrative Code 216](#).

B. **Roles**

1. **Information Resource Manager (IRM):** An individual appointed by the University President to oversee the acquisition, operation, and support of University information resources (see [Texas Administrative Code 211.20: Selection of Information Resources Managers](#)). The IRM is ultimately responsible for the management of the institutions information resources. Partners with the CISO, University IROs, IRCs, and P-ISAs to successfully lead and coordinate the institution's information resource activities.

2. **Chief Information Security Officer (CISO):**An individual other than the IRM appointed by the University President to oversee the University's information security program as defined in [Texas Administrative Code 202.71(d)](#). Responsible for recommending and developing security policies, procedures, and practices in coordination with the IRM, IROs, IRCs, and P-ISAs; maintaining an up-to-date security program; monitoring and reporting on the effectiveness of defined information resource security controls; and approve exceptions to information security controls.

3. **Information Resource Officer (IRO):** A role designated by the office's vice president or dean to coordinate and/or delegate the development of strategies, plans, procedures, and security for the offices's information resource assets, projects, and compliance activities. The individual that performs this role will coordinate the activities of the IRC and P-ISA or may perform the IRC and P-ISA roles. The IROs designated by the offices of the University, together with the IRM and the CISO, will form the IRM Advisory Board that will be involved in drafting university-wide information technology policies and advise the IRM in the creation and design of information technology strategies, plans, and procedures.

4. **Information Resource Coordinator (IRC):** A role designated by the offices's vice president or dean to coordinate and/or delegate the daily operations of IT activities and projects within the office. The individual that performs this role may also perform the IRO and P-ISA roles or will coordinate with these individuals. The IRCs designated by the offices of the University, together with a representative designated by the IRM, will form the IRC Advisory Board which will be involved in the development of operational strategies and best practice recommendations for daily IT activities and projects and will advise the IRM in decisions regarding university-wide information resource development and information technology projects.

5. **Principal Information Security Administrator (P-ISA):** A role designated by the office's vice president or dean to coordinate and/or delegate the implementation of the UT Arlington Information Security Program for the college or administrative office in compliance with [UTS 165](#). The P-ISA is distinguished from the office's ISAs (whose role is defined in UTS 165), as this role will be sufficiently empowered by the office's dean or vice president to implement and/or coordinate the information security activities for the entire office. The individual that performs this role may also perform the IRO and IRC roles or will coordinate activities with these individuals. The P-ISAs designated by the offices of the university, together with the CISO and a representative designated by the IRM, will be members of the Information Security Advisory Committee that will be involved in the drafting of university-wide information security policies and advise the CISO in the creation and design of information security programs, procedures, and initiatives.

C. **Information Resource Coordination Support**
The Office of Information Technology (OIT) will support offices in coordinating information resources as outlined in Section II. A by providing the following consultative, best practice services:

1. Facilitation and coordination of university-wide planning for information resource management as outlined in Section II. A

2. Information technology governance activities including facilitation of regular meetings for IROs and IRCs

3. Training of office's information technology support staff

4. Access to information resource management tools and services

5. Procedures, practices, and reference materials

6. Assistance with office's information technology initiatives

D. **Information Security Coordination Support**
The Information Security Office (ISO) will support offices in implementing UT Arlington's Information Security Program as outlined in UTS 165.

E. **General Provisions**

1. OIT will provide training, information, and consultation (upon request) to facilitate office compliance with this policy.

2. Offices will conduct reviews and updates (as needed) of information resource management procedures.

III. **Definitions**

The definitions found in this section are to be interpreted consistently with other definitions in Texas Administrative Code 202, University of Texas System 165, and other policies found the Handbook of Operating Procedures covering Information Technology and Security. Where definitions do not exist in this policy, the definitions shall be derived from those policies or regulations.

Administrative Office: An office led by an administrative officer (vice president, dean, or academic office chair) charged with overseeing specific administrative functions of the University (see *Duties of Administrative Officers*(Policy 2-100)).

IV. **Relevant Federal and State Statutes**

Gramm-Leach-Bliley Act (GLBA)

Family Educational Rights and Privacy Act (FERPA)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry (PCI) Data Security Standard

Texas Administrative Code - Information Security Standards (1 TAC 202)

Texas Administrative Code - Project Management Practices (1 TAC 216)

Texas Administrative Code, Title 1, Part 10, Chapter 211, Subchapter C; Selection of Information Resource Managers

[Texas Government Code, Chapter 2054, "Information Resources"](#)

V. **Relevant UT System Policies, Procedures and Forms**

[Office of Information Technology Supported Hardware](#)

[Office of Information Technology Supported Software](#)

Duties of Administrative Officers ([Policy 2-100](#))

Business Continuity Policy ([Policy 5-306](#))

Best Value Procurement ([Policy 5-403](#))

Information Technology and Security Policies ([Policy 5-600](#))

Records and Information Management ([Procedure 13-5](#))

Removal of Property from a Department's Inventory([Procedure 2-45](#))

[UT System Administration Policy UTS165: UT System Information Resource Use and Security Policy](#)

[UT System Information Security Program Elements](#)

VI. **Who Should Know**

Vice presidents, deans, and all employees involved in the management and support of information resources.

VII. **UT Arlington Office(s) Responsible for Policy**

Office of Information Technology

VIII. **Dates Approved or Amended**

November 20, 2014

IX. **Contact Information**

Chief Information Officer and Vice President of Information Technology

cio@uta.edu817-272-5602