
I N T R O D U C T I O N

This 2006 Action Plan to Enhance Information Security Compliance (2006 Information Security Action Plan) is to address the high risk area of Information Security Compliance and is an enhancement to 1998 and 2003 Action Plans to Ensure Institutional Compliance within The University of Texas System (UT System).

The mission statement of the Institutional Compliance program is “The University of Texas System (U.T. System) endeavors to fulfill all of its responsibilities to the people of Texas in an environment based upon ethical behavior and compliance with applicable laws and rules.” The two primary goals of the program are:

- ❖ providing assurance that all faculty and staff are aware of their duties and responsibilities in establishing and sustaining that environment; and
- ❖ providing a mechanism for continuously assessing the effectiveness of that environment in assuring that all UT System activities are conducted with integrity.

The purpose of the 2006 Information Security Action Plan is to address the ongoing elements of an effective compliance program in information security to minimize the risk of significant compliance failures and enhance compliance through best practices. General guidance is provided for Information Security Compliance in the UT System Business Procedures Memorandum 53-06-05 Information Resources Use and Security Policy and the Texas Administrative Code Part 10, Chapter 202 Information Security Standards (TAC 202).

The following pages present the 2006 Information Security Action Plan items by “Responsible Party.” The Action Plan includes the following key elements:

- The designation of the System-wide Chief Information Security Officer (CISO).
- The designation of an appropriate Information Security Officer (ISO) at U. T. System Administration, each institution and UTIMCO. The ISO should report to the institutional Information Resources Manager (IRM) and the System-wide CISO.
- The establishment of a System-wide Information Security Council that meets at least quarterly and parallel Information Security Working Committees at U. T. System Administration, each institution, and UTIMCO that meet at least monthly.
- The mandate for a *continuous and proactive* compliance program that reports to the Compliance Officer at System Administration, each component institution, and UTIMCO.
- The allocation of sufficient resources at U. T. System Administration, each institution, and UTIMCO to fund compliance activities (including staffing, training, and monitoring activities) that reduce compliance risk to a reasonably low level.

The 2006 Information Security Action Plan assigns responsibility and accountability for compliance with laws, regulations, policies, and procedures as follows:

- The System-wide CISO will provide leadership, strategic direction, and coordination for the system-wide information security initiative. The System-wide CISO is responsible and will be held accountable for apprising the Chancellor and the Board of Regents of the information security compliance programs and activities at System Administration, each of the institutions, and UTIMCO.
- The ISOs at U. T. System Administration, each institution, and UTIMCO are responsible and will be held accountable for information security for all centrally maintained and distributed systems and computer equipment. The ISO reports to the Institutional IRM. An auxiliary reporting relationship to the System-wide CISO exists for purposes of conducting CIO Council business and maintaining compliance communications. Responsibility for actual compliance with laws, regulations, policies, and procedures rests with each individual employee. Accountability resides primarily with the department head of each operating unit.
- The Chancellor and each Chief Administrative Officer are responsible and will be held accountable for the sufficiency of resources allocated to information security compliance activities and the appropriateness of

corrective and disciplinary action taken in the event of non-compliance.

This action plan has been shared with the Strategic Leadership Council on June 1, 2006 and was submitted to the Audit, Compliance, and Management Review Committee (“ACMR”) of the UT Board of Regents on August 9, 2006. Questions about the 2006 Information Security Action Plan should be directed to Charles G. Chaffin, System-wide Compliance Officer (512-499-4390).

ACTION PLAN – INFORMATION SECURITY COMPLIANCE

| Action | Responsible Party | Due Date |
|--|---|----------|
| 1. Designate an executive officer at The University of Texas System as the System-wide Chief Information Security Officer, with authority and responsibility for guidance, direction, and oversight of the System-wide Information Security Program. | Chancellor | |
| 2. Designate an Information Security Officer (ISO) at System Administration, each institution and UTIMCO reporting to the System-wide Chief Information Security Officer and to the institutional IRM with the authority and responsibility for the institution’s Information Security Program. | Chancellor Chief Administrative Officer Chief Information Officer | |
| 3. Establish The UT System Information Security Council composed of the ISOs from System Administration, each institution, and UTIMCO that is chaired by the UT System-wide Chief Information Security Officer. Require the Information Security Council to meet at least quarterly. | Chancellor System-wide Chief Information Security Officer | |
| <p><i>Implementation Guidance: Consideration will be given to the utilization of already established working groups to fulfill this action step. The Information Security Council should facilitate policy setting and governance, communication and sharing of ideas, best practices, exposures, and other information related to information security risks.</i></p> | | |
| 4. Develop a System-wide Information Security Compliance program, as well as, full-scale Information Security Compliance programs at System Administration, each institution and UTIMCO. | Institutional Information Security Officers | |
| The System-wide Information Security Officer, with assistance from the System-wide Compliance Officer, will have the authority and responsibility for program oversight. This program would include System-wide, as well as, institutional action plans, training plans, and monitoring plans. | System-wide Chief Information Security Officer Institution Compliance Officer | |

| Action | Responsible Party | Due Date |
|--|---|----------|
| <p>5. Budget sufficient resources to fund ongoing and continuous information security remediation, implementation, and compliance activities (staffing, training, tools, and monitoring activities) that reduce compliance risk to an acceptably low level.</p> <p><i>Implementation Guidance: The System-wide Chief Information Security Officer will explore the acquisition of tools and resources that can be utilized system-wide and how expertise can be shared among institutions.</i></p> | <p>Chancellor Chief Administrative Officer</p> | |
| <p>6. The System-wide Chief Information Security Officer will establish a standardized risk assessment methodology to be utilized system-wide. System Administration, each institution, and UTIMCO shall conduct and document an information security risk assessment annually in accordance with TAC 202.72 that identifies significant and critical information assets in both central and decentralized areas. Ensure an information security risk assessment is performed by each information owner of significant and/or critical information assets in the institution on an annual basis.</p> <p><i>Implementation Guidance: This action step addresses the assessment of the risks associated with high-risk areas as defined by TAC 202.72. TAC 202.72 indicates that all high-risk information resources must be subjected to an annual risk assessment. High-risk Resources must be identified as significant and/or critical information assets based on the results of data classification. As identified in the requirements of BPM 75 section 3.2, each institution may use its own classification guidelines to satisfy the data classification requirement. However, at least one data classification category must include a direct correlation to TAC 202.72's high-risk information resources definition. The risk assessment results may differ between the institutions depending on the nature of the operations.</i></p> | <p>Institutional Information Security Officer</p> <p>System-wide Chief Information Security Officer</p> <p>System-wide Compliance Officer</p> | |
| <p>7. Require the owners of significant and/or critical information assets at System Administration, each Institution and UTIMCO to designate a person responsible for security of the system or asset with the knowledge and training to receive and distribute time-critical computing and security-related information. This person (Information Security Administrator) will be responsible for the implementation of and compliance with all Information Technology policies and procedures and for reporting general computing and security incidents to the ISO.</p> | <p>Institutional Information Security Officer</p> | |
| <p>8. Establish an Institutional Information Security Working Group at System Administration, each institution, and UTIMCO chaired by the Information Security Officer, and composed of the Information Security Administrators. Require the Institutional Information Security Working Group to meet</p> | <p>Institutional Information Security Officer</p> | |

| Action | Responsible Party | Due Date |
|--|--|----------|
| <p>monthly and to maintain records of its meetings.</p> <p><i>Implementation Guidance: The Institutional Information Security Working Group should assist the Information Security Officer in developing, implementing and monitoring the Information Security Program.</i></p> | | |
| <p>9. Document and maintain an up to date Institutional Information Security Program which details the specific mitigation strategies to be used by each information owner of significant and/or critical information assets in the institution to manage risks identified in step #6. The information security program must be approved by the Chief Administrative Officer or his or her designated representative(s).</p> <p><i>Implementation Guidance: The plan developed for TAC 202 could be expanded to include the required information. Guidance on the plan including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards will be provided by the System-wide Chief Information Security Officer. Revise current BPMs related to information security.</i></p> | <p>System-wide Chief Information Security Officer</p> <p>Institutional Information Security Officer</p> | |
| <p>10. Ensure that high-level information security training is included in first-time General Compliance Training and in every subsequent update for all employees. Ensure that specialized, detailed training is provided to information owners and Information Security Administrators on an annual basis. Ensure that all Information Security Officers and Information Security Administrators are properly trained on information security requirements and applicable governance documents (TAC 202, BPMs, etc).</p> <p><i>Implementation Guidance: Training should be coordinated with the Institutional Compliance Officer and use of already established training delivery systems should be considered.</i></p> | <p>Institutional Information Security Officer</p> <p>Institutional Compliance Officer</p> | |
| <p>11. Establish reporting guidance, metrics, and timelines for the Institutional Information Security Officer to monitor effectiveness of security strategies in both the centralized and decentralized operations.</p> <p>Establish reporting guidance, metrics, and timelines for the System-wide Chief Information Security Officer to monitor effectiveness of security strategies at System Administration, each institution, and UTIMCO.</p> <p><i>Implementation Guidance: Reporting guidance, metrics, and timelines should consider already established statutory reporting requirements to reduce duplication of effort and the results of the</i></p> | <p>Institutional Information Security Administrators</p> <p>Institutional Information Security Officer</p> <p>System-wide Informational Security Officer</p> | |

| Action | Responsible Party | Due Date |
|---|--|----------|
| <i>risk assessment performed in step #6.</i> | | |
| <p>12. The Information Security Officer shall report, at least annually, to the Chief Administrative Officer or his or her designated representative(s) and the System-wide Chief Information Security Officer on the status and effectiveness of information resources security controls.</p> <p><i>Implementation Guidance: The report should also include the status of the information security risk assessment, that there are appropriate strategies being applied consistently to manage the identified risks, and whether all security breaches have been reported.</i></p> | <p>Institutional Information Security Administrators</p> <p>Institutional Information Security Officer</p> <p>System-wide Informational Security Officer</p> | |
| <p>13. The Institutional Compliance Officer will provide high-level monitoring of the Information Security Program through inspections and verifications of reported information as part of their normal oversight of high risk areas.</p> | <p>Institutional Compliance Officer</p> | |
| <p>14. Internal audit may conduct audits of the Information Security Program as part of their normal assurance services or special agreed-upon-procedures as part of their consulting services.</p> | <p>Internal Audit</p> | |
| <p>15. The System-wide Information Security Officer will report activity quarterly to the Audit, Compliance, and Management Review Committee of the Board.</p> | <p>System-wide Informational Security Officer</p> | |

Definitions:

Information Resources Manager (IRM): The IRM is responsible for management of all of the institution’s information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the institution including both centralized and decentralized systems. If an agency does not designate an IRM, the title defaults to the institution’s president, and the president is responsible for adhering to the duties and requirements of an IRM.

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.