The Division of Information Technology
University Information Security Standards

Information Security Standard – Internet Usage (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas and must be managed as valuable state resources. This procedure is established to achieve the following:

1.1 To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

1.2 To establish acceptable practices regarding the use of information resources; and,

1.3 To educate individuals who may use information resources with respect to their responsibilities associated with such use.

2. Applicability

This standard applies to all University information resources.

The purpose of this standard is to provide a set of measures that will mitigate information security risks associated with Internet/Intranet use. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience is all users of University information resources.

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2 Information Resources: 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 assistant (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.

3.3 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

4. Procedures

4.1 All files downloaded from the Internet/Intranet shall be scanned by software to safeguard against viruses, malware, and malicious code. Procedures regarding the protection of information resources against viruses, malware, and malicious codes; web site standards, and personal conduct can be found in the following policies and procedures:

Rules for Responsible Information Technology Usage, 33.04.99.W1/PR
Security of Electronic Information Resources, 24.99.99.W1/PR
System Policy 07.01, Ethics Policy
University Rule, Web Accessibility and Usability

4.2 University Internet access may not be used for personal gain or solicitations.

4.4 No university mission critical or confidential information shall be made available via university websites or public websites without ensuring that the material is accessible to only authorized individuals or groups.

4.5.1 All mission critical or confidential information transmitted over external networks must be encrypted.

4.5.2 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with University records retention schedules.

4.5.3 Division heads, directors, and department heads or their equivalent have the responsibility to ensure that appropriate security practices for West Texas A&M University Internet/Intranet use are implemented in their respective departments.

4.7 Any security violations, and all signs of wrongdoing pertaining to this procedure, shall be reported according to the University Incident Management standard administrative procedure.

4.8 Incidental use of Internet/Intranet access is subject to University Rules for Responsible IT Usage, 33.04.99.W1/PR.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer