Scope

All individuals accessing The University of Texas at Tyler's information or information systems including without limitation employees, faculty, students, visitors, volunteers, contractors, and vendors, and to all University computers or other information resources owned, leased, administered, or otherwise in the custody and control of the University, wherever located.

Purpose

To provide internet website and mobile application security procedures, as required by Section 2054.517 of the Texas Government Code.

POLICY

The University's Information Security Officer (ISO) is responsible for developing and implementing the policy and procedures in conjunction with the University's Office of Legal Affairs, Privacy Officer, and other officials responsible for compliance with privacy laws (including HIPAA and FERPA) and data security laws. The policy and procedures should consider business processes such as contracting, acceptance testing, and system deployment, etc.

(a) Before deploying an Internet website or mobile application that processes confidential information for the University, the developer of the website or application must submit to the ISO the information required under University policies adopted to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the developer must submit information describing:

    (1) the architecture of the website or application;

    (2) the authentication mechanism for the website or application; and

    (3) the administrator level access to data included in the website or application.

(b) Before deploying an Internet website or mobile application, the Data Owner must subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party. The cost of the vulnerability and penetration test will be the responsibility of the Data Owner. Review and acceptance of the findings shall comply with UTS 165 Standard 10.8.

(c) The Information Security Office will assist the Data Owner in collecting the information required and acquiring the appropriate testing services. The Software Purchase Checklist will not be approved until the required information and testing has been completed.

(d) The University will submit a copy of this policy to the Texas Department of Information Resources for review and recommendations for appropriate changes. The ISO is responsible for ultimate content of the policy.

Violation of UTS 165 or other U. T. System or University Information Security Policies or Standards by faculty, staff, and students who have access to U. T. System Information Resources or Data for the purpose of providing services to or on behalf of the University will subject those individuals to disciplinary action in accordance with the applicable University policies. For contractors and consultants, this may include termination of the work engagement and execution of penalties contained in the work contract. For volunteers, this may include dismissal. Additionally, certain violations may result in civil action or referral for criminal prosecution.

References

- Texas Government Code, Section 2054.517
- University of Texas System Policy UTS 165, Standard 11.8