UTSA Institutional Compliance Office of Information Security

OIS-43 – Standard for Application Administrator

I. STANDARD STATEMENT

This standard defines the duties of an application administrator.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. DEFINITIONS

on a regular basis - at least annually

VI. PROCEDURES

A. Application Administrator

1. The application administrator must perform a vulnerability scan, or ensure the Office of Information Security performs a vulnerability scan for Web applications:
   a. Prior to moving the application to the Production environment
   b. After a compromise of the Web application
   c. On a regular basis, for all mission-critical operations
   d. As requested by the application owner when potential or existing risks are identified within the environment
2. The application administrator must complete a risk assessment on a regular basis, as specified in the Standard for Information Security Risk Assessment.
3. The application administrator must complete a data review prior to moving the application to the Production environment
   a. Any request to access or use application data must be approved by the data owner.
   b. Data owner should be notified if data is to be stored outside of the university
   c. If the data is to be hosted outside of UTSA, an agreement must be reviewed by the UTSA Purchasing and Legal departments and the Office of Information Security.

B. Application Developer or Application Acquisition Team
   1. Follow standard for granting access to the application, as specified in the Standard for Account Management (OIS-1).
   2. Identify all confidential information and document the business need for having that data.
   3. Provide safeguards to protect data from exposure.
   4. Encrypt all data in transit.
   5. Identify all data owners, data custodians and system administrators.
   6. Ensure the application validates input, executes proper error handling and authenticates users through identity management processing if local authentication is supported.
   7. Include information security, security testing and audit controls in all phases of the development/acquisition process.
   8. Institute a change control process so the data owner approves all security-related information resources changes.
   9. Ensure the application enforces passphrase requirements as described in the Standard for Passwords and Passphrases (OIS 25).

C. University Technology Solutions (UTS) Staff Member
   1. Create and maintain the Application Registry. Ask for the following:
      a. Purpose of the application
      b. Staff members responsible for the application
      c. Data classification
      d. Relevant technical information
   2. Enforcement of this policy.
   3. Perform audits and monitoring activities to detect any unsecured systems.
   4. Provide technical assistance to departments so they can meet the requirements.

D. Policy Review
   1. In order to maintain currency of the Information Security Program, this policy is subject to review by the Office of Information Security on a regular basis.
   2. Any exception to requirements set forth in this policy must be approved in writing by the UTSA Office of Information Security.

Title: OIS-43 Standard for Application Administrator
Effective Date: September 12, 2014
Last Reviewed: August 12, 2020