TITLE: Information and Computer System Classification Procedures

NUMBER: INF100

EFFECTIVE: 14 MAR 2014

REVIEWED: 26 MAR 2015

PURPOSE: To provide a mechanism whereby all information and computer systems under institute purview are classified as to sensitivity to the use of and storage of information in order to mitigate risks associated with compromised information or systems. This procedure is established to meet the requirement of UT Policy IT0115 – Information and Computer System Classification.

PROCEDURES:

1. Information Owners and Information System Owners will:
    a. Identify and document the information types stored or processed on each system;
    b. Select the security impact levels and security category for identified information types;
    c. Document the provisional impact levels associated with the system's information type;
    d. Review the appropriateness of the provisional impact levels based on organizational guidance and document adjustments to the impact levels;
    e. Determine and assign the security categorization by identifying the highest security impact level;
    f. Select and implement the appropriate controls for each system from NIST SP 800-53 "Recommended Security Controls for Federal Information Systems and Organizations" using the baseline controls established by the Statewide IT Governance Program and with the cooperation of the campus/unit Information Security Officer;
2. On an annual basis:
    a. Provide to the Chief Information Security Officer at the institute a single report detailing:
        i. System identification information;
        ii. Types of information stored on the system;
        iii. Security impact levels of the system;
        iv. Security category for information type;
        v. Provisional Impact Levels associated with the system ;
        vi. Ensure the system has been reviewed on an annual basis for
    b. The Chief Information Security Officer will provide a consolidated report to institute and the UTSA Chief Information Officer ensuring the guidelines laid forth in UT Policy IT0115 and this procedure have been met.

DEFINATIONS:

1. Information Owners are defined as the individual with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal
2. Information System owners within the Institute for Public Service are Identified as Lisa Shipley (MTAS), Jon Walden (CTAS), John Erdmann (CIS), and Scott Gordy (IPS Administrations, Naifeh Center, and LEIC).

RELATED POLICIES:

UT IT0115 – Information and Computer System Classification

UT IT0121 - Information Security Plan Creation, Implementation, and Maintenance.

RESOURCES:

IPS Security Plan

CONTACT:

Scott Gordy, 865.974.4944, scott.gordy@tennessee.edu