OIS 47 – Standard for Information Security Administrators

I. STANDARD STATEMENT

The program for Information Security Administrators (ISAs) is designed to complement the information security program and augment the protection of data and computing resources by identifying, training and assisting qualified representatives in the departments of the university. The responsibilities of the ISAs are established in UTS 165, UT System Information Resources Use and Security, Section 1.7.

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. Responsibilities

A. ISAs who manage a single machine that stores confidential data (for example, research data). The ISA will:

1. Ensure antivirus software is installed and is up to date and a full antivirus scan is performed on a weekly basis
2. For UTSA-owned and managed computers, antivirus software is installed and maintained automatically
3. Ensure the computer has the latest Operating System updates
4. For UTSA-owned and managed computers, operating system updates are installed automatically
5. Ensure the data on the primary computer is being backed up. At UTSA, CrashPlan is the preferred software application.
6. Ensure that the computer, if it is a laptop, is encrypted

7. Ensure that the computer, if it is a desktop, is encrypted if it is classified as a Category I machine, or if it was purchased after September 1, 2013

B. ISAs who manage a shared information resource. The ISA will
   1. Conduct an initial inventory – with the assistance of the Data Owner (DO) – of software, hardware and secured facilities under his/her responsibility to OIS.
   2. Review the Access Control Lists (ACL), consisting of (at minimum) names of individuals and their general level of access to resources.
   3. Review and update the inventory list and/or the ACLs when changes occur in the department.
   4. As a member of the ISA work group, assist the ISO in developing, implementing and monitoring the Information Security Program.
   5. Establish reporting guidance, metrics and timelines for the ISO to monitor effectiveness of security strategies in both the centralized and decentralized operations.
   6. Report on a regular basis to the ISO on the status and effectiveness of information resources security controls.

VI. PROCEDURES

A. Information Security Administrator (ISA)
   1. Implements and complies with all information technology policies and procedures relating to assigned systems.
   2. Performs, on a regular basis, an Information Security Risk Assessment for key Information Resources, as determined by the ISA and OIS.
   3. Reports general computing and Security Incidents to the UTSA Information Security Officer (ISO), in the time frame specified.
   4. ISAs may also hold the role of Data Custodians.
   5. If the ISA is also a server administrator, the ISA must comply with the Server Administrator Policy.

B. ISO
   1. Approves the appointment of all ISAs.
   2. Requires that each ISA performs an annual Information Security Risk Assessment.
   3. Holds regularly scheduled meetings with ISAs to discuss information security. Meetings are scheduled and ISAs are notified of the meeting times.
   4. Ensures that ISAs are adequately trained on information security requirements.
   5. Works with the Data Owners to ensure compliance with the Data Owner Policy.

C. Data Owner
   1. Assigns one or more ISAs in support of their Data Owner responsibilities.
   2. Ensures ISA(s) perform(s) Information Security Risk Assessment(s) on a regular basis.
   3. Holds regularly scheduled meetings with ISAs to discuss information security.

D. Data Custodian
   1. Implements and complies with all information technology policies and procedures relating to assigned systems, including those required to maintain compliance with all metrics defined in the InSight application.

2. Implements the controls specified by the Data Owner(s).
3. Provides physical, technical and procedural safeguards for the Information Resources.
4. Backs up Data in accordance with risk management decisions and secures Backup media.
5. Assists Data Owners in evaluating the cost-effectiveness of controls and monitoring.
6. Implements monitoring techniques and procedures for detecting, reporting and investigating Security Incidents.

Effective Date: September 11, 2014
Last Revised: October 12, 2014
Last Reviewed: August 10, 2020