OIS- 41 Standard for Position of Trust

I. STANDARD STATEMENT

The University of Texas at San Antonio (UTSA) relies significantly on a wide variety of Information Resources to achieve its missions. The UTSA Office of Information Security (OIS) and University Technology Solutions (UTS) are responsible for administering programs that create a reliable and secure UTSA computing environment. In order to maintain the security and integrity of the computing infrastructure, every effort must be made to protect the Data, intellectual property and Information Resources used to carry out UTSA business.

II. RATIONALE

Individuals placed in a Position of Special Trust by their department are granted elevated administrative privileges to UTSA Information Resources and therefore have a greater responsibility to ensure no harm comes to the Information Resources or Data by the use of those privileges.

III. SCOPE

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

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. A person in a position of special trust must ensure that all of the systems for which they are responsible are in compliance with InSight application metrics, including but not limited to:
   1. Must have antivirus software installed and updated.
   2. Must meet all encryption standards.
   3. Must be reporting to the InSight application.
   4. Must be a member of the Active Directory domain.
   5. Must have all approved patches/updates installed.

B. Individuals in a position of special trust should:
   1. Document areas of concern and present to management.
   2. Only use high level / administrative access when required. All other times use your normal levels of access.

3. Participate in specialized training, as assigned.
4. Dot "I's" and cross "T's" when working with high level access or "Tools of Mass Disruption."
5. Carelessness and negligence in positions of special trust will not be tolerated.

C. Elevated Access Privileges.
   1. Elevated access privileges are granted to those individuals who require the ability to access resources that are usually restricted from standard users.
   2. If an elevated access privilege account is compromised, an unauthorized user could cause serious harm to the computer network. Therefore, this type of account should only be used to access the required resources. For all other activities, the user should log on using their regular user account.

D. General Listing of Systems that Require a Position of Special Trust Form to be completed by users.
   1. While some systems may have been inadvertently omitted, the following systems / platforms require a POST form to be completed by those with access:
      a. PeopleSoft/DEFINE administrators
      b. Banner Administrator, Database Administrator, Programmer
      c. Blackboard Administrator
      d. Network Administrator

E. Positions of Special Trust Acknowledgement Form
   1. Prior to providing access to a system covered by this policy or its related standards, the manager authorizing access will notify employee that it requires a Positions of Special Trust Acknowledgement Form to be completed. Managers needing assistance in determining whether a Positions of Special Trust Acknowledgement Form is required may contact OIS.
   2. Employee in Positions of Special Trust should review this policy, the acknowledgement form and other related resources.
   3. The manager/department will retain the form.
   4. The Positions of Special Trust Acknowledgement Form should be completed annually by employees designated as being in a Position of Special Trust.

F. General procedures for Users in a Position of Special Trust
   1. Exercise special care in carrying out work so as to prevent errors that may be costly or adversely affect UTSA Users.
   2. Recognize and address the possibility of such errors and follow all defined procedures with extra diligence.
   3. Use accounts with special privileges (e.g., System Administrators, Database Administrators, and Network Administrators) only for their intended administrative purposes.
   4. Make immediate supervisor aware of issues or process defects which should be addressed to minimize risks of disruption of information services or Data breach.

G. Definitions

"Immediately informs" - The user will inform management as soon as possible.

H. The form is available at:

https://utsacloud.sharepoint.com/:w:/s/Security/oispublic/Ee5Nax6whIRNuEcm9azDWjwB8bNA3U4ib1ispXH3gKEnaA?e=9Qcmgs

Title: OIS-41 Standard for Position of Trust
Effective Date: September 11, 2015
Last Revised: August 12, 2020