UTSA Institutional Compliance Office of Information Security

OIS 44 – Standard for Data Owners

I. STANDARD STATEMENT

Data Owners are custodians responsible for protecting and monitoring access to data - a vital information resource.

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

A. **Mission Critical Information Resources** - Information Resources defined by an Entity to be essential to the Entity's function and that, if made unavailable, will inflict substantial harm to the Entity and the Entity's ability to meet its instructional, research, patient care, or public service missions. Mission Critical Information Resources include Confidential Data.

B. **Mission-Critical Systems** - The following applications have been identified as mission critical. [Note: This is not a comprehensive list.]

1. Ellucian Banner Student
2. ASAP Student Portal
3. Blackboard Learn
4. Early Alert System (EAS)
5. Course Leaf Catalog Management System
6. Global Advising system
7. UC Event/Class Scheduler (R25)
8. PeopleSoft – HMS
9. PeopleSoft – FMS
10. HVAC IT Services
11. Library IT Services
12. Testing IT Services

VI. PROCEDURES

A. General Procedure

1. Data Owners will refer to the Standard for Data Classification for determining the level of protection needed for their data.
2. For matters pertaining to access management, the Data Owner should refer to the Standard for Account Management.
3. The Data Owner has specific duties in regard to Risk Assessment. These duties can be found in the Standard for Information Resources Risk Assessment.
4. Risk assessments will be performed annually.
5. Account access reviews will be performed annually.
6. Meetings with Information Security Administrators (ISAs) to discuss information security will be held at least annually.

B. Data Owner General Procedure
1. Data Owners will use physical controls, software and other methods to protect and monitor access to Data and/or systems that host that Data.
2. Data Owners, Data Custodians and Users of Information Resources will be identified, and their responsibilities defined and documented.
3. In cases where Information Resources are used by more than one major business function, the Data Owners will reach consensus and advise the ISO of the designated owner responsible for the Information Resources.
4. Any changes to the data schema (adding or removing data elements) must be reviewed and approved by the Data Owner.
5. The Data must be retained based on the Data Retention period set out in UTSA's Records Retention Schedule (link).
6. University Data must not be stored on personally-owned devices.

C. Access Management
1. All accounts that access UTSA information must be managed according to access management principles as specified in the Standard for Account Management. The level of authorized access for an individual account must be based on the Principle of Least Privilege - that is, an individual may be granted access to only the information needed to perform the required duties.
2. All accounts will be uniquely identifiable and will be assigned to an individual. Account names may not be re-assigned or changed under any circumstances.
3. Accounts will be changed to reflect the modification of privileges if an employee or a student changes roles within the University.
4. Commensurate with risk and reasonable practice, accounts must be reviewed regularly to ensure currency of the privileges.
5. Password aging and expiration dates must be enabled for all special accounts granted to outside vendors, contractors and those with contractually limited access.

D. Information Security Risk Assessments
1. Departments and data owners who manage Information Resources must sponsor formal risk assessments to identify potential problems that may affect the operation and security of assigned Information Resources.

2. The staff members who perform the Information Security Risk Assessment will work with the Data Owner/department head and OIS to identify controls that will provide protection and/or recovery from loss, exposure or inappropriate modification of the Data.
3. The strategy report that results from the Information Security Risk Assessment will be submitted to the ISO and will cover the planning and control for the most critical risks.
4. The ISO will incorporate the strategy reports into a university-wide framework and provide a copy to the Executive Compliance Committee (ECC) or President as required.
5. Information Security Risk Assessments will be performed on a regular basis at an appropriate unit level, summarized and provided to upper organization levels.
6. The Data Owner will review and update the Information Security Risk Assessment on a regular basis. ISAs will provide assistance as needed.

7. Copies of the Information Security Risk Assessments, updates and executive summaries will be provided to OIS.

Title: OIS 44- Standard for Data Owners
Effective Date: September 4, 2014
Last Reviewed: August 12, 2020