ITS Service Management System Policy

Version: 1.2
Effective Date: 12/17/2019

Policy Summary:

This policy defines how the Information Technology and Security (ITS) Service Management System (SMS) will be planned, established, implemented, operated, monitored, reviewed, maintained and improved. This establishes senior staff commitment to ensure a set of capabilities and processes that direct and control the activities and resources for the planning, design, transition, delivery and improvement of technology services that deliver value.

Questions regarding this policy should be directed to the Managing Director, IT Operations at 813-257-3277.

Applicability/Eligibility:
This policy applies to all staff managing and maintaining technology services provided by Information Technology and Security (ITS). The scope of the Service Management System may be amended based on the needs of the University.

Exceptions:
None

Policy Administration:

Mandating Authority: (Check all that apply)

☐ Federal Law
☒ University President
☒ Other: (ISO Stds)
☐ State Law or Regulation
☐ Accrediting Body

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology and Security, Managing Director of IT Operations	East Walker Hall 121	813-257-3277

Responsible Executive(s):

Name	Title	Phone Number
Tammy Clark	Vice President, Information Technology and Security	813-257-7522

Policy Management:

Policy History:

Date	Version	Reason for Change
08/17/2019	1.0	Initial policy draft
12/10/2019	1.2	Aligned the policy with other ISO management systems for a combined audit.

Policy Approvals and Reviews:

Date	Organizational Group
12/17/2019	President
12/17/2019	Senior Staff

Web Links:

Policy Link: https://www.ut.edu/sms

Full Policy Text:

Information Technology and Security (ITS) Service Management System (SMS):

Leadership. Senior staff shall demonstrate leadership and commitment with respect to the ITS service management system.

Planning. Information Technology & Security will develop an annual ITS service management plan.

Risk Management. ITS will complete risk assessments using ISO/IEC 27005:2011 - Information Security Risk Management and the National Institute of Standards and Technology's Special Publication 800-53, Security and Privacy Controls for Federal Systems and Organizations.

Service Requirements. A clear definition of ITS service requirements will be agreed upon and maintained by senior staff of all ITS services so that ITS service management activity is focused on the fulfillment of those requirements. The provision of ITS services is driven by university needs and will be regularly communicated to the university community.

Implementation and Management. The ITS service management system manager will have responsibility for the implementation and management of the SMS.
Specifically:

a) The identification, documentation, and fulfillment of service requirements
b) Assigning responsibility for the implementation, management, and improvement of service management processes
c) Reporting to top management of the performance and improvement of ITS services

Delivery of Services by Other Parties. Various third parties are used both internal and external in the delivery of ITS services. External suppliers will be managed through service level agreements and the associated underpinning contract. Internal providers will be managed through operational level agreements (OLA).

In all cases ITS will retain governance of the relevant processes by demonstrating:

a) Accountability for the process
b) Control of the definition of the interface to the process
c) Performance and compliance monitoring
d) Control over process improvements

This will be evidenced by documents and records such as contracts, OLAs, meeting minutes, and performance reports.

Document Control. Relevant versions of applicable documents will be available at points of use. Documents housed in the ITS SMS documentation library need to be labeled and controlled in accordance with the ITS SMS documentation standard. ITS departments are responsible for managing and updating their procedures and documentation in the ITS SMS documentation library each year.

Internal Audit. Internal audits of the ITS service management system shall be conducted annually. Personnel who are independent of the current work or project shall be retained to perform internal audits.

Management Reviews. Management reviews will be conducted by ITS at various intervals.

Non-conformity and corrective actions. ITS service management system nonconformities and corrections will be documented and maintained by ITS.

ITS departments notified about corrective actions must submit a corrective action plan to the SMS manager within 30 days. A notable exception is that corrective actions resulting from British Standards Institution (BSI) certification audits must be submitted within 15 days, to provide time for the BSI auditor to accept the corrective action plan(s).

Records Retention. Unless specified otherwise, ITS service management system records will be maintained electronically by ITS for a minimum of three (3) years.

Training. All ITS departments included in the service management system scope shall be made aware of the relevance and importance of their service management activities and how they contribute to the achievement of goals and objectives. ITS will provide training for the ITS service management system participants.

Additional Information and Resources:

Reference:

ISO/IEC 20000-1:2018 (E) Societal security – Service management systems. Geneva, Switzerland: ISO/IEC.

Definitions:

ISO/IEC 20000:2018 Certification. A three-stage external audit process defined by the ISO/IEC 17021 and ISO/IEC 27006 standards:

- Stage 1 is a preliminary, informal review of the SMS that familiarizes certification auditors with the organization and vice versa.
- Stage 2 is a more detailed and formal compliance audit, independently testing the SMS against the requirements specified in ISO/IEC 20000:2018. Successful completion of this stage results in the ISMS being certified compliant with ISO/IEC 20000:2018.
- Stage 3 involves follow-up reviews and audits to ensure the organization remains in compliance with the standard.

Non-conformity. The certification audit will grade the audit criteria as ‘conforms or nonconforms.’ There are two types of non-conformities:

- Major Nonconformity - A major breakdown or failure to fulfill one or more requirements of the SMS.
- Minor Nonconformity - A single identified lapse, which would not raise significant doubt as to the capability of the SMS to achieve the service objectives of the organization.