THE UNIVERSITY OF TAMPA
INFORMATION TECHNOLOGY AND SECURITY

ITS Service Management System Policy

Version: 1.2
Effective Date: 4/25/2023
Last Reviewed: 11/11/2024

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 ITS Leadership 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 UTCIO@ut.edu.

Applicability/Eligibility:

This policy applies to Information Technology and Security (ITS) Leadership, Service Desk and Technical Support staff. 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 Standards)
☐ State Law or Regulation
☐ Accrediting Body

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology and Security, AVP Enterprise Solutions	Jenkins Technology Building, Room 381B	813-257-3218
Information Technology and Security, AVP IT Operations	Jenkins Technology Building, Room 381D	813-257-5372

Responsible Executive(s):

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

Policy Management:

Policy History:

Date	Version	Reason for Change
03/27/2023	1.0	Initial policy draft
4/8/2024	1.1	Updated language to reflect standard for internal audits.
11/11/2024	1.2	Updated Senior Staff to President's Cabinet

Policy Approvals and Reviews:

Date	Organizational Group
4/25/2023	President
4/25/2023	Senior Staff
12/3/2024	

Web Links:

Policy Link: Service Management Policy

Full Policy Text:

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

Leadership. The ITS Leadership team shall demonstrate management and commitment with respect to the ITS service management system, including a commitment to continuously improving the SMS and its services.

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

Risk Management. A risk management strategy and process will be used which is in line with the requirements and recommendations of ISO/IEC 27005:2022, the international standard for risk management.

Implementation and Management. The ITS service management system manager(s) 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

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 (i.e., contracts, OLAs, meeting minutes, performance reports, etc.).

Document Control. Relevant versions of applicable documents will be available. 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 ensure objectivity and the impartiality of the audit process.

Management Reviews. Management reviews will be conducted by ITS at least annually.

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(s) 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 team members 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.

Definitions:

ISO/IEC 20000:2018 Certification. A three-stage external audit process defined by the ISO/IEC 19001:2018:

- 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.

ITS Service Catalog. It is a storefront from where the UT community can request ITS services and products from the ITS Service Desk based on the information provided in the service catalog.

Service Management System. Service management is a customer-focused approach to delivering information technology and security services. Service management focuses on providing value to the customer and on the customer relationship.

Service Level Agreement (SLA). A service-level agreement (SLA) defines the level of service you expect from a vendor, laying out the metrics by which service is measured, as well as remedies or penalties should service levels not be achieved. It is a critical component of any technology vendor contract. The SLAs are reviewed as part of the vendor scorecard process with both the vendor and key campus stakeholders.

Operational Level Agreement (OLA). Internal agreements that ITS defines with key campus stakeholders to accomplish one or more key objectives and/or service targets. These results are reviewed on a recurring basis to determine if there's a need for modification for continuous improvement.