The University Of
TAMPA

Information Security Management System Policy

Version: 3.0
Effective Date: 3/29/2016

Policy Summary:
This policy establishes the top management commitment to satisfy International Organization for Standardization/International Electro-technical Commission's ISO/IEC 27001:2013 requirements for developing an effective Information Security Management System. The information security management system's scope of participation at UT is incremental and will continue to be scaled in accordance with University requirements.

Questions about this policy should be directed to the VP. Information Technology and Security at infosec@ut.edu or (813) 257-7522.

Applicability/Eligibility:
This policy applies to UT Organizations that are included within the scope of the information security management system: (Information Technology & Security, Human Resources, and Sykes COB ITM Cybersecurity Academic Program – Faculty & Staff)

Exceptions:
None

Policy Administration:

Mandating Authority:
(Check all that apply)

☐ Federal Law
☐ State Law or Regulation
☐ University President
☐ Accrediting Body
☐ Other: (specify)

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology & Security	East Walker Hall Rm 133	813-257-7522

Responsible Executive(s):

Name	Title	Phone Number
Tammy L. Loper	VP, Information Technology and Security	813-257-7522

Policy Management:

Policy History:

Date	Version	Reason for Change
2/18/2014	1.0	Initial Policy
12/8/2015	2.0	Scope Change
2/8/2016	3.0	Corrective Action and Documentation Requirements

Policy Approvals and Reviews:

Date	Organizational Group
3/29/16	President
3/29/16	Senior Staff
3/14/22	Changed Last name of VP from Clark to Loper. No other changes

Web Links:

Policy Link: Information Security Management System Policy

Full Policy Text:

Information Security Management System requirements:

Leadership. Top management shall demonstrate leadership and commitment with respect to the Information Security Management System.

Planning. *Information Technology & Security* (ITS) will develop an annual information security 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.

Statement of Applicability. *ITS* will document the information security controls selected for implementation, identify progress, and provide justification for exclusions.

Document Control. Relevant versions of applicable documents will be available at points of use. Documents housed in the ISMS documentation library need to be labeled with the organization, Appendix A control, and title of the document (ex. IT – 17.1.1 – Business Continuity Plan). Organizations are responsible for managing and updating their procedures and documentation in the ISMS documentation library each year.

When a new procedure, or version of a procedure, is issued for inclusion in the information security management system it will include:

1. A revision level showing the new document(s)/version(s)
2. Point(s) of contact for questions or comments
3. Date of last update or issuance
4. Data classification (if sensitive or confidential)

Internal Audit. Internal audits of the information security 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. Information security management system nonconformities and corrections will be documented and maintained by *ITS.*

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

Corrective action plans will be managed by the ITS PMO.

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

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

Definitions:

ISO/IEC 27001:2013 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 ISMS that familiarizes certification auditors with the organization and vice versa.
- Stage 2 is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001:2013. Successful completion of this stage results in the ISMS being certified compliant with ISO/IEC 27001:2013.
- Stage 3 involves follow-up reviews and audits to ensure the organization remains in compliance with the standard.

Information Security Management System. The governing principle behind an ISMS is that an organization should design, implement, and maintain a coherent set of policies, processes, and systems to manage risks to its information assets, thus ensuring acceptable levels of risk.

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

- Major Nonconformity—A major breakdown or failure to fulfill one or more requirements of the ISMS

- Minor Nonconformity—A single identified lapse, which would not raise significant doubt as to the capability of the ISMS to achieve the security standards and objectives of the organization