THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0115 - Information and Computer System Classification	
Version: 2	**Effective Date: 10/01/2017**

IT0115 - Information and Computer System Classification

Objective:

To establish policy for information and computer system classification.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee including its campuses, institutes, and administration (University and/or Campuses).

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program that demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University IT resources.

Policy:

Each Campus must develop or adopt and adhere to a formal documented program for the categorization of information and information systems according to risk level by applying guidance found in FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volumes I and II.

Responsibilities:

Information Owners and Information System Owners will:

1. Identify and document information types stored or processed by each information system.
2. Select the security impact levels and security category for identified information types.
3. Document the provisional impact levels associated with the system's information type.
4. Review the appropriateness of the provisional impact levels based on organizational guidance (see Definitions), and document adjustments to the impact levels.
5. Determine and assign the security categorization by identifying the highest security impact level.
6. Select and implement appropriate controls for each system from NIST SP 800-53 "Recommended Security Controls for Federal Information Systems and Organizations" using the baseline established by the Statewide IT Governance

Program and with the cooperation of the campus/unit Information Security Officer.

Special Notes:

Certain special provisions and requirements, that apply to information classification, are provided to ease the interpretation and implementation process.

1. The university, except as recognized in the Statement of Policy on Patents, Copyrights, and Licensing retains ultimate ownership of all information.
2. To ensure proper protection of the university's information, any information or computer system not otherwise classified is presumed to be at least: "FIPS199 Security Category = {(confidentiality: Low), (integrity: Low), (availability: Low)}".
3. Computer systems meeting the criteria of multiple classification levels must protect the highest level of information on the system or a detailed plan must be provided detailing a clear separation of data and the protections for each classification of data on the system.
4. All computer systems that handle, process, or store the university's information at an offsite location must adhere to this policy. Contracts with third-party vendors that handle, process, or store the university's information should reflect a requirement that they acknowledge and adhere to this policy.

References:

1. Federal Information Processing Standards Publication 199: Standards for Security Categorization (FIPS199)
2. National Institute of Standards and Technology (NIST) Special Publications (SP)
   a. 800-53
   b. 800-60 Volume I
   c. 800-60 Volume II

Definitions:

1. **Information Owner** - Individual with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
2. **Information System Owner** - Individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
3. **Information System** - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
4. **Information Type** - A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization, or in some instances, by a specific law, policy, or regulation.
5. **Organizational Guidance** - A campus or institute-specific document that provides guidance for categorizing specific information types (for example: Confidential Information.)
6. **Security Categorization** - The process of determining the security category for information or an information system. Security categorization methodologies are described Federal Information Processing Standard (FIPS 199) and National Institute for Standards and Technology (NIST) SP 800-60.

Last Reviewed: January 13, 2016