

<b>UT Space Institute Policy:</b>	
<b>IT0115-SI – Information and Computer System Classification Plan</b>	
<b>Version: 1</b>	<b>Effective Date: 10/06/2019</b>

### **Objective**

To establish a formal, documented plan for classifying business-critical information and computer systems.

### **Scope**

This plan applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee Space Institute (UTSI) including its remote centers.

“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 and Technology (NIST) 800 series of publications, and this policy is based on those guidelines. This plan is based on guidelines in NIST SP 800-60 Volumes I and II and the Federal Information Processing Standards Publication 199 (FIPS 199).

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.

UTSI must develop or adopt and adhere to a plan that demonstrates compliance with related policies and standards. This plan 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 University policy is assumed if a User accesses, uses, or handles University resources.

### **Plan Details**

Security categorization provides a structured method for determining the criticality and sensitivity of the information processed, stored, and transmitted by an information system. The security categories of Low, Moderate, and High are based on the potential impact to an organization should certain events occur that jeopardize the organization’s ability to continue its day-to-day functions. The security category and security impact level of the information system must be recorded in the UTSI System Classification and Risk Assessment sheet.

This plan applies to all IT systems under the responsibility of UTSI personnel. A list of these systems can be found in the UTSI System Classification and Risk Assessment sheet.

<b>UT Space Institute Policy:</b>	
<b>IT0115-SI – Information and Computer System Classification Plan</b>	
<b>Version: 1</b>	<b>Effective Date: 10/06/2019</b>

## **Roles and Responsibilities**

Chief Information Officer. Has overall accountability of this plan as the Position of Authority. Also responsible for specifying servers as business-critical.

IT Administrator. Responsible for:

- Identifying and documenting information types stored or processed by each information system.
- Selecting the security impact levels and security category for identified information types.
- Documenting the provisional impact levels associated with the system's information type.
- Reviewing the appropriateness of the provisional impact levels based on organizational guidance (see Definitions), and document adjustments to the impact levels.
- Determining and assigning the security categorization by identifying the highest security impact level.
- Selecting and implementing 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

## **Adverse Effects Definitions**

A limited adverse effect is characterized by:

- degradation in mission capability and effectiveness of primary functions
- minor damage to University assets
- minor financial loss

A serious adverse effect is characterized by:

- significant degradation in mission capability and effectiveness of primary functions
- significant damage to University assets
- significant financial loss

A severe or catastrophic adverse effect is characterized by:

- severe degradation in or loss of mission capability and inability to perform primary functions
- major damage to University assets
- major financial loss

<b>UT Space Institute Policy:</b>	
<b>IT0115-SI – Information and Computer System Classification Plan</b>	
<b>Version: 1</b>	<b>Effective Date: 10/06/2019</b>

## Categorization

Information and information systems are categorized according to risk level by applying guidance found in FIPS 199 and NIST SP 800-60 Volumes I and II. FIPS 199 establishes security categories for both information and information systems while the NIST SP 800-60 volumes contain basic guidelines for mapping types of information and information systems to security categories and recommendations and rationale for various information types.

UT Policy IT0115 - *Information and Computer System Classification* requires campuses to classify information systems with the potential impact categories (low, moderate, or high) for the three information security objectives (confidentiality, integrity, and availability).

Information System and Information Classification			
Security Objective	Potential Impact		
	Low	Moderate	High
<b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b> Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Availability</b> Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

## Categorization Process

### Identify information types

- The IT Administrator should identify all of the types of information processed, stored, or transmitted by the information system.



# SPACE INSTITUTE

<b>UT Space Institute Policy:</b>	
<b>IT0115-SI – Information and Computer System Classification Plan</b>	
<b>Version: 1</b>	<b>Effective Date: 10/06/2019</b>

## Select Initial Impact Level and Adjust

- Select impact levels (low, moderate, high) using the original impact levels assigned to the security objectives (confidentiality, integrity, availability) for each information type (see Appendix A for guidance).
- Review the appropriateness of the security impact levels and adjust, if necessary.

## Assign System Security Category

- Determine the system security category based on the highest level of security objective for each information type.

## Document the Process and Results

- Categorization information must be recorded in the UTSI System Classification and Risk Assessment sheet.

## **Special Notes**

The following special provisions and requirements that apply to information classification are provided to ease the interpretation and implementation process:

- The university, except as recognized in the Statement of Policy on Patents, Copyrights, and Licensing retains ultimate ownership of all information.
- To ensure proper protection of the university's information, any information or computer system not otherwise classified is presumed to be at least: "FIPS 199 Security Category = {(confidentiality: Low), (integrity: Low), (availability: Low)}".
- 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.
- 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.

<b>UT Space Institute Policy:</b>	
<b>IT0115-SI – Information and Computer System Classification Plan</b>	
<b>Version: 1</b>	<b>Effective Date: 10/06/2019</b>

## References

FIPS 199 - *Standards for Security Categorization of Federal Information and Information Systems*

NIST SP 800-53 Rev 4 - *Recommended Security Controls for Federal Information Systems and Organizations*

800-60 Volume I Rev 1 - *Guide for Mapping Types of Information and Information Systems to Security Categories*

800-60 Volume II Rev 1 - *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*

## Definitions

Availability - Ensuring timely and reliable access to and use of information.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, destruction, or loss of information or information system availability.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

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.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Organizational Guidance - A campus or institute-specific document that provides guidance for categorizing specific information types (for example: Confidential Information.)

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.

Security Category - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.



# SPACE INSTITUTE

<b>UT Space Institute Policy:</b>	
<b>IT0115-SI – Information and Computer System Classification Plan</b>	
<b>Version: 1</b>	<b>Effective Date: 10/06/2019</b>

## Appendix A - Guidance for Categorizing Information Types

Data Type	Confidentiality	Integrity	Availability
General	Low	Low	Low
Student Data (FERPA controlled)	Moderate	Moderate	Low
Academic Transcripts			
Student Biographical Information			
Scholarship Information (with student name)			
Grades			
Course Schedule (with student name)			
Advising Notes (with student name)			
Procurement, credit, or debit card numbers (non-PCI)	Moderate	Moderate	Low
PCI	Moderate	Moderate	Low
Payroll	Low	Moderate	Low
Point of Sale (POS) Transactions	Low	Moderate	Moderate
Personally Identifiable Information (PII)	Moderate	Moderate	Low
Legally Protected	Moderate	Moderate	Low
Change Management Information	Low	Moderate	Low
System Maintenance Information	Low	Moderate	Low
IT Infrastructure Maintenance Information	Low	Low	Low
Information Security Information	Low	Moderate	Low
System and Network Monitoring Information	Moderate	Moderate	Low