# CONTENTS

1. **Scope** ................................................................................................................. 2
2. **Principles** ........................................................................................................... 2
3. **Revisions** ........................................................................................................... 2
4. **Objective** ........................................................................................................... 2
5. **Policy** ................................................................................................................ 2
6. **Systems Under Information & System Classification Control** ......................... 3
7. **Responsibilities** ............................................................................................... 3
8. **Classification Guide** ....................................................................................... 4
9. **Definitions** ....................................................................................................... 7
10. **IT Security Office** .......................................................................................... 7
1. **Scope**

This Guide applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Chattanooga.

“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.

2. **Principles**

This document is a University of Tennessee at Chattanooga-specific Guide based on University policy. Each User of UTC resources is required to be familiar and comply with University policies, and acceptance is assumed if the User accesses, uses, or handles UTC information technology resources.

The Associate Vice Chancellor and Chief Information Officer (AVC/CIO) is responsible for information technology and security at the University of Tennessee Chattanooga. The AVC/CIO is the Position of Authority (POA) for Information Technology at UTC.

3. **Revisions**

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/20/2017</td>
<td>Version 1.0</td>
<td>Michael Dinkins</td>
</tr>
</tbody>
</table>

4. **Objective**

This document provides guidance for developing, maintaining and documenting an Information and System Classification program for UTC’s business-essential information systems.

5. **Policy**

This guide is a supplement to published University of Tennessee Policy IT0115, Information and System Classification. Click here for more information. The policy requires UTC to develop or adopt and adhere to a formal, documented information
and information system classification program that provides effective information and information system controls.

6. Systems Under Information & System Classification Control

A formal Information and Systems Classification program must be applied to the following functional systems/subsystems:

<table>
<thead>
<tr>
<th>MISSION-ESSENTIAL SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Banner</td>
</tr>
<tr>
<td>Banner</td>
</tr>
<tr>
<td>Banner</td>
</tr>
<tr>
<td>Enterprise Services (Non-Banner)</td>
</tr>
<tr>
<td>Infrastructure</td>
</tr>
<tr>
<td>Infrastructure</td>
</tr>
<tr>
<td>Moderate-categorized Departments</td>
</tr>
</tbody>
</table>

7. Responsibilities

<table>
<thead>
<tr>
<th>ROLE</th>
<th>RESPONSIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Vice-Chancellor &amp; CIO (AV/CIO)</td>
<td>As Position of Authority (POA), the AVC/CIO has overall responsibility of the Information and Systems Classification program for business-critical systems at UTC. The AVC/CIO Technology Advisory Team must ensure:</td>
</tr>
<tr>
<td></td>
<td>1) The Information &amp; System Classification program is developed, documented, and disseminated in accordance with University policy.</td>
</tr>
<tr>
<td></td>
<td>2) The Information &amp; System Classification program is reviewed and updated annually.</td>
</tr>
</tbody>
</table>
3) Critical business systems and mission-essential functions are identified for Information & System Classification program inclusion.

**Chief Information Security Officer**

The CISO and IT Security Team consults and assists the CIO and systems owners of business-critical systems to ensure:

1. Information and systems are properly classified in accordance with UT Policy.
2. Appropriate procedures are implemented, reviewed and updated annually.

**Subsystem Owner / Administrator (or assignee)**

System owners are responsible for developing, maintaining and disseminating procedures for their respective system(s) per the following Classification Guide. Owners of MODERATE-classified systems and information should:

1. Assign an IT Security Liaison to work with the IT Security Team on security issues and communications between the department and IT Security Office.
2. Create a Systems Security Plan in which all IT Security-related documents can be stored, accessed and referenced.
3. Document the classification of data and review their information types annually.
4. In the EXAMPLE below, the UTC Department that owns the information type listed is classified MODERATE because at least one type of information is classified as MODERATE for Confidentiality, Integrity or Availability.

---

**8. Classification Guide**

Information and information systems are classified 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.

**FIPS 199 Publication**

The FIPS 199 provides guidance on how an organization can establish security categories for both information and information systems. The security categories LOW, MODERATE, and HIGH are based on the potential impact on an organization should certain events occur which jeopardize the organization’s ability to continue its day-to-day functions.
At UTC, the IT Security Office has initially classified all department in which users work with sensitive information (e.g. Social Security Numbers, FERPA, Credit Card, HIPAA, etc.) as having MODERATE impact should there be a breach of data. Owners of MODERATE-classified information/systems must ensure stricter security controls and best practices are implemented in their organization. IT Security recommends the department assign an IT Security Liaison to work with the IT Security Team and build and system security action plan to meet security goals.

Per UT Policy IT0115, all department Information and Information System Owners will:

- Identify and document information types stored or processed by each information system.
- Select the security impact levels and security category for identified information types.
- Document the provisional impact levels associated with the system's information type.
- Review the appropriateness of the provisional impact levels based on organizational guidance (see Definitions), and document adjustments to the impact levels.
Determine and assign the security categorization by identifying the highest security impact level.

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.

In the EXAMPLE below, the UTC Department that owns the information type listed is classified MODERATE because at least one type of information is classified as MODERATE for Confidentiality, Integrity or Availability.

**EXAMPLE: HOW TO CATEGORIZE INFORMATION**

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Confidentiality (HIGH/MOD/LOW)</th>
<th>Integrity (HIGH/MOD/LOW)</th>
<th>Availability (HIGH/MOD/LOW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative - General</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Administrative - PII</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Administrative - PCI</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>DEPARTMENT CLASSIFICATION</td>
<td>MODERATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SPECIAL NOTES**

Certain 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: "FIPS199 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.

9. 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.

10. **IT Security Office**

    Michael Dinkins, CISSP  
    Chief Information Security Officer  
    (423)425-4507  
    michael-dinkins@utc.edu  

    Larry Prince  
    IT Security Analyst  
    (423)425-2904  
    larry-prince@utc.edu