## CONTENTS

1. **Scope** ................................................................................................................................. 2
2. **Principles** ............................................................................................................................. 2
3. **Revisions** ............................................................................................................................ 2
4. **Objective** ............................................................................................................................. 2
5. **Policy** ................................................................................................................................. 2
6. **Applicability** ........................................................................................................................ 3
7. **Responsibilities** .................................................................................................................. 3
8. **IT Security Office** ............................................................................................................... 5
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>4/14/2017</td>
<td>Version 1.0</td>
<td>Michael Dinkins</td>
</tr>
</tbody>
</table>

4. **Objective**
This document provides guidance for developing, maintaining and documenting a System & Information Integrity program for UTC’s business-critical information systems.

5. **Policy**
This guide is a supplement to published University of Tennessee Policy IT01xx, System & Information Integrity. Click here for more information. This policy requires UTC to
develop and adhere to a formal, documented System & Information Integrity program that addresses:

- Flaw Remediation
- Malicious Code Protection
- Information System Monitoring
- Spam Protection
- Information Handling and Retention

6. Applicability

A formal System & Information Integrity program must be applied to the following functional systems/subsystems:

<table>
<thead>
<tr>
<th>MISSION-ESSENTIAL SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</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 registered with Office of CIO</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 AV/CIO has overall responsibility for the System &amp; Information Integrity (SI) program. The AV/CIO ensures:</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Chief Information Security Officer | The CISO is responsible for overseeing the implementation of the UTC System & Information Integrity (SI) program for systems that support mission-essential functions. The CISO and IT Security Team consults and assists systems owners to ensure:  
1) An SI program is in effect and the departments develop, document and disseminate procedures necessary to facilitate the implementation of the System & Information Integrity policy.  
2) Information system flaws are addressed and remediated in a timely manner.  
3) Appropriate tools are employed to monitor threats to the Information system.  
4) Malicious code protection is employed, current and periodically assessed.  
5) Appropriate systems employ spam protection.  
6) A documented process is established for information handling and retention.  
7) The System & Information Integrity program is reviewed and updated annually. |
| Subsystem Owner / Administrator (or assignee) | System owners are responsible for developing procedures and/or processes for their respective system(s) ensuring:  
1) **Flaw Remediation.** Regularly assess systems for flaws and address identified issues in a timely manner, and apply relevant software and firmware updates at the earliest appropriate maintenance cycle. *Critical flaws may require an emergency update between normal maintenance cycles.*  
2) **Malicious Code Protection:**  
a) Employ latest malicious code protection mechanisms to detect, block, quarantine, or eradicate malicious code, and alert administrative staff.  
b) Periodically scan critical information systems for malicious code.  
3) **Information System Monitoring:** Use appropriate tools and methodology to:  
a) Monitor systems and networks for indicators of attacks, and unauthorized connections. |
b) Assess identified indicators and report unauthorized activity to the Security Incident Response Team (SIRT) via the Help Desk.

4) **Spam Protection**: Employ the use of appropriate tools, practices and staff training in order to minimize spam.

5) **Information Handling and Retention**: Develop, document and maintain a process/procedure for information handling and retaining the out of your system in accordance with applicable federal and state laws, and University policies, standards, and requirements. This includes devices that produce hardcopy output (e.g. printers and fax machines).

---

### 8. 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