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...............................................................................................4
9. Definitions..........................................................................................................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>4/28/2017</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 Audit and Accountability Program for the University of Tennessee at Chattanooga’s business-critical information systems.

5. Policy
This guide is a supplement to published University of Tennessee Policy IT0127, Audit and Accountability. Click here for more information. The policy requires UTC’s Audit
and Accountability program to include procedures that address the following controls for business-critical systems:

1) Determining auditable events.
2) Audit records management.
3) Procedures for:
   a. Response to audit processing failures.
   b. Log review, analysis and reporting.

6. Applicability

A formal Audit and Accountability 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>-------</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 AVC/CIO has overall responsibility of the Audit &amp; Accountability program at UTC. The AVC/CIO ensures:</td>
</tr>
</tbody>
</table>
1) The Audit & Accountability program is developed, documented, and disseminated to appropriate UTC entities in accordance with University policy.

2) The program is reviewed and updated annually.

3) Critical business systems and mission-essential functions are identified for inclusion in the program.

Chief Information Security Officer

The CISO is responsible for overseeing the implementation of the UTC Audit & Accountability program for systems that support mission-essential functions. The CISO and IT Security Team consults and assists the CIO and systems owners of business-critical systems to ensure:

1) Creation of procedures that address:
   a) Auditable events.
   b) Audit records management.
   c) Response to audit processing failures.
   d) Log review, analysis and reporting.

2) Procedures are reviewed/updated annually.

Subsystem Owner / Administrator (or assignee)

System owners are responsible for developing and documenting procedures for their respective system(s) ensuring:

1) Determination and documentation of which auditable events are deemed significant and relevant to the security of the system. Examples of auditable events include (but not limited to) system, application, network, and user activity.

2) Ensuring audit record management procedures address:
   a) Generation of audit records that include the type of event, when it occurred, where it happened, source of the event, outcome and associated system and/or individual(s).
   b) Record protection.
   c) Record retention.

3) Event alerting and response.

4) Log review, analysis, and reporting.

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
9. Definitions

1) **Audit Event** is any observable occurrence in an organizational information system.

2) **Audit record content** includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames.

3) **Audit storage capacity.** Allocating sufficient audit storage reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

4) **Audit review, analysis, and reporting** can include, for example, results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, component inventory, use of maintenance tools, physical access, and use of VoIP. Findings can be reported to the IT Security Incident Response Team and/or Help Desk.

5) **Audit record retention.** Audit records must be retained until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes.