OBJECTIVE

All university computer systems, regardless of classification, must be protected from unauthorized interruption of service. The COMPUTER SYSTEM CLASSIFICATION POLICY (IT0116) assigns a level of responsibility to the Computer System Custodian for evaluating and assigning the appropriate computer system classification to all computer systems for which they are responsible. This policy provides guidelines to evaluate and assign the appropriate classification to all computer systems. It defines:

- A standard framework for categorizing computer systems according to their relative importance or effect on the operational goals of the university.
- Clear responsibility for identifying and implementing required security protections based on the designated classification.
- A methodology to establish and create controls that limit the effects of planned or unplanned interruptions of service to any computer system.

SCOPE

Individuals Covered
This policy applies to all students, faculty, staff, and others—referred to as “users” throughout this policy—who access, use, or handle the university’s IT resources. "Users" include but are not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities or individuals who are granted access.

Resources Covered
This policy applies to all university IT resources, whether individually controlled, shared, stand-alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or provided by the university or otherwise connected to university IT resources. This includes but is not limited to networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, whether used for administration, research, teaching, or other purposes. This policy also applies to all personally owned devices used to store, process, or transmit university information or that are otherwise connected to university IT resources.
COMPLIANCE
At minimum, individual university units (e.g. campuses or institutes, departments, colleges, and divisions) must follow these principles and rules while connected to university IT resources. Each unit is responsible for security on its systems and may apply more stringent security standards than those detailed here, provided these do not conflict with or lower standards or requirements established by the IT security strategy, policies, or best practices.

Any non-compliance with the university’s IT security strategy, policies, or best practices must be reported to the position of authority (POA) or their designee for IT at the respective campus/institute or the Information Security Office (ISO). The contact information for both entities, the ISO and the POA, can be found at http://security.tennessee.edu/. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. The ISO will work with Human Resources and Student Judicial Affairs to develop and implement appropriate sanctions for non-compliance. Issues that cannot be resolved by the ISO will be directed to the Vice President for Information Technology. Critical non-compliance issues will be directed to the Audit Committee of the Board of Trustees.

GENERAL POLICY
RESPONSIBILITIES
1. The following roles and responsibilities for installing, managing, and sanitizing the university's computer systems establish the hierarchy for compliance with this policy.
   a. **Computer System User**: anyone using university computer system as a part of his or her job or other university-related activity. User responsibilities include:
      i. Follow the operating procedures defined by the computer system custodian or manager.
      ii. Comply with university information security policies and best practices to insure the availability of the computer system.
      iii. Use the university's computer systems only for approved purposes.
      iv. Report suspected violations of policies and best practices to the POA or the ISO.
      v. Report suspected breached or compromised security to the computer system custodian or manager.

   b. **Computer System Manager**: anyone delegated to maintain security controls by the computer system custodian. Manager responsibilities include:
      i. Administer computer system protection controls as directed by the computer system custodian.
      ii. Provide protection that maintains access to the university computer system.
      iii. Based on guidance from the computer system custodian,
1. Detect and respond to violations and vulnerabilities.
2. Monitor compliance with computer system and information security policies and best practices.
   iv. Report non-compliance with university policies and best practices to the POA or the ISO.
   v. Report suspected breached or compromised security to the computer system custodian.

c. **Computer System Custodian**: the employee assigned responsibility for specific university computer systems. Custodian responsibilities include:
   i. Classify the assigned computer system(s).
   ii. Establish the necessary controls to protect the availability of the computer system.
   iii. Implement information systems security policies and best practices to protect the computer system.
   iv. Define and establish the appropriate business use of the computer system.
   v. Determine the requirements to authorize access to the computer system.
   vi. Communicate control and protection requirements to computer system managers and users.
   vii. Report non-compliance with university policies and best practices and suspected or actual breached or compromised security to the Information POA or the ISO.

d. **Information Security Officer**: the person who maintains this policy and ensures that the computer system custodian has the infrastructure necessary to establish and maintain appropriate security controls.

2. The following special provisions and requirements should ease interpretation and implementation of this policy.
   a. Any computer system not otherwise classified is presumed to be "Non-critical," as defined in the following section.
   b. Computer systems that perform operations in multiple classification levels must be protected to the highest classification level.
   c. All computer systems that handle, process, or store the university's information at an offsite location must adhere to this policy.
   d. Custodians may classify a computer system at a higher level than the definition allows, if the risk to the university is consistent with the classification.

**Computer System Classifications**
University computer systems are classified into three categories based, upon the expected adverse effect each will have on university operations, university assets, or individuals if the system becomes unavailable.
3. **Non-critical**: Disrupted access to or use of the computer system(s) could be expected to have a *limited* adverse effect on university operations, university assets, or individuals.

   a. The computer system(s) is necessary for university operation; however, unplanned long-term interruption of service is acceptable. The system
      i. Plays no direct or a significantly indirect role in the key operational activities of the university.
      ii. Presents no danger to the health, security, or safety of individuals.

   b. **Evaluation Criteria**
      Planned interruptions – **Acceptable**
      Unplanned short-term interruptions – **Acceptable**
      Unplanned long-term interruptions – **Acceptable**

      **No or limited**
      • Effect on university operations, university assets, or individuals
      • Effect on research or instruction
      • Financial effect on the university
      • Potential legal ramifications for the university
      • Effect on contractual obligations for the university
      o Loss of strategic advantage for the university

4. **Critical**: Distributed access to or use of the computer system(s) could be expected to have a *serious* adverse effect on university operations, university assets, or individuals.

   a. The computer system(s) is required to perform a critical university operation. Unplanned short-term interruption of service is acceptable.
      i. Business continuity plans must address unplanned long-term interruptions so as to maintain operations until the systems are fully restored.

   b. **Evaluation criteria**
      Planned interruptions – **Acceptable**
      Unplanned short-term interruptions – **Acceptable**
      Unplanned long-term interruptions – **Unacceptable**

      **Serious**
      • Effect on university operations, university assets, or individuals
      • Effect on research or instruction
      • Financial effect on the university
      • Potential legal ramifications for the university
      • Effect on contractual obligations for the university
      • Loss of strategic advantage for the university

5. **Highly Critical**: Disrupted access to or use of the computer system(s) could be expected to have a *severe or catastrophic* adverse effect on university operations, university assets, or individuals.
a. The computer system(s) is required to perform a critical university operation. Unplanned interruption of service is unacceptable.
   i. Systems must resume operation within a very short time, following interrupted service.
   ii. Business continuity plans must address interruptions where service does not resume within a defined timeframe so as to maintain operations until systems are restored.

b. Evaluation Criteria

<table>
<thead>
<tr>
<th>Planned interruptions</th>
<th>Acceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unplanned short-term</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>interruptions</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>Unplanned long-term</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>interruptions</td>
<td></td>
</tr>
</tbody>
</table>

**Severe or catastrophic**

- Effect on university operations, university assets, or individuals
- Effect on research or instruction
- Financial effect on the university
- Potential legal ramifications for the university
- Contractual obligations for the university
- Loss of strategic advantage for the university

**CLASSIFICATION DOCUMENTATION PROCESS**

Classification documentation must be created and maintained for all computer systems, clearly identifying the computer system custodian, manager(s), and users and their respective responsibilities as well as the requirements for protecting the system.