Audit Policy

1. **Overview**
    a. The purpose for this policy is to encourage the usage of Information Assurance policies. The Security Officer can and will conduct audits at given times to gauge the current state of involved ISAT assets. Faculty and staff are encouraged to review policies on a regular basis. Instructors can encourage students to review and practice some or all policies.
2. **Purpose**
    a. The main reasons for an audit policy are:
        i. It establishes the need to analyze the state of the network and its components.
        ii. It may help mitigate some risk as found by an audit.
        iii. It encourages faculty, staff, and students to reassess Information Assurance and ISAT security policies.
3. **Responsibility**
    a. The Security Officer is responsible for performing audits on all or portions of ISAT equipment. All ISAT faculty, staff, and entities working on behalf of Southern Illinois University Carbondale are subject to usage of the Information Assurance policies to ensure that audits will provide results that reinforces Information Assurance. Students are also encouraged to develop similar strategies.
4. **Scope**
    a. All ISAT faculty and staff computer and communication devices owned or operated by Southern Illinois University Carbondale.
    b. All ISAT lab computers and network devices.
    c. The ISAT will not perform Denial of Service activities or disruptive audits.
5. **Action**
    a. Run software audits using Microsoft Assessment and Planning Toolkit on ISAT computer systems to ensure that licensing is in check. Investigate non-compliance.
    b. Run network discovery scans on ISAT networks to ensure that connected equipment belongs to Southern Illinois University Carbondale.
    c. All ISAT faculty, staff, and entities working on behalf of Southern Illinois University Carbondale are encouraged to review policies on an annual basis.
    d. Instructors can inform and encourage students to review policies starting each new semester.
6. **Enforcement**
    a. Any employee found to have violated this policy may be subject to disciplinary action, in accordance with University policies and procedures.

7. **Definitions**
    a. Microsoft Assessment and Planning Toolkit (MAP) – An agentless software suite from Microsoft that auto-discovers Microsoft operating systems as well as Linux-based and VMware operating systems on a network. It performs a software inventory as well as provides utilization statistics for Microsoft systems.
    b. Security Officer – This individual is appointed by the College as the person that monitors and keeps record of both infractions and established standards of the College in the area of information systems network security.
8. **Revision History**
    a. Policy is in effect on 01/01/2011
    b. Document revised on 11/19/2010
        i. Revised by Michael Garrison