Incident Response Policy

1. **Overview**
    - **a.** The purpose for this policy is to establish a procedure for dealing with computer security incidents. ISAT employees must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident. All employees should familiarize themselves with the guidelines of this policy.
2. **Purpose**
    - **a.** The main reasons for a incident response policy are:
        - **i.** Provide ISAT support personnel with guidelines on what to do if they discover a security incident.
        - **ii.** Provide guidelines to protect information and systems.
        - **iii.** Provide guidelines for the containment and eradication of the problem.
        - **iv.** Provide guidelines for recovering from the incident and the follow-up analysis.
3. **Responsibility**
    - **a.** All faculty, staff, and entities working on behalf of Southern Illinois University Carbondale are subject to usage of this policy. Students are also encouraged to develop similar strategies.
4. **Scope**
    - **a.** All ISAT computer, peripheral devices, and network assets are affected by this policy.
    - **b.** Violation of security policies is considered a security incident.
    - **c.** General security-related incidents should be reported regardless of severity.
5. **Action**
    - **a.** Students should report incidents to instructors. If the incident happens outside of a classroom setting, students should notify Security Officer.
    - **b.** Faculty, staff, and entities working on behalf of Southern Illinois University Carbondale should report incidents directly to Security Officer
    - **c.** Affected systems should be isolated immediately until the problem cause can be established.
    - **d.** A root cause investigation should be conducted and return a cause and effect analysis.
    - **e.** Systems should be returned to normal operating modes once the problem has been eradicated.
    - **f.** All incident information should be documented and maintained by the Security Officer.
    - **g.** Documented incidents should include the nature of the incident, action taken to contain and resolve, as well as the results of the root cause investigation.

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. Root Cause Investigation – The process of identifying the primary event that led to the security incident. The purpose is to establish an action plan for dealing with the incident as well as preventing a repeat, if possible.
    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 11/17/2010
        i. Revised by Michael Garrison