Physical Security Policy

1. **Overview**
    - **a.** The purpose for this policy is to establish a culture of security and trust for all faculty, staff, and students. An effective physical security effort involving the participation and support of all Southern Illinois University Carbondale employees can greatly protect electronic documents that contain protected information about our students, customers and vendors. It also will protect against theft or misplacement. All employees and students should familiarize themselves with the guidelines of this policy.
2. **Purpose**
    - **a.** The main reasons for a physical security policy are:
        - a.i. It reduces the threat of a security incident as protected information will be secured when unattended.
        - a.ii. Protected documents saved on unsecured workstations can be stolen by a malicious entity or mistakenly misplaced/deleted by unauthorized users.
        - a.iii. Reduces the likelihood of University assets disappearing due to theft or misplacement.
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 physical assets purchased by the University that are subject to registration and tagging by the University's Fixed Assets department.
    - **b.** Areas (e.g. labs, offices) that hold equipment that falls within the other scopes of this document.
5. **Action**
    - **a.** All physical assets purchased by the University shall be registered and tagged by the University's Fixed Assets department.
    - **b.** All physical assets that are portable enough to be carried out of the building easily and are used either as lab equipment or might contain protected information on them (e.g. desktop computers, laptops) should be secured using security cables and padlocks.
    - **c.** For equipment that is too small or where part of its intended use requires portability, the asset should be stored in a locked cabinet.
    - **d.** Common areas (e.g. labs) should have some sort of video surveillance to help ensure equipment is not taken or moved by unauthorized individuals.
    - **e.** Access to locked assets by students should require the approval of either an instructor or member of staff that is responsible for the asset (e.g. Network Administrator).
    - **f.** Any offices that contain physical assets should remain locked when unattended. Access to such offices should only be granted by authorized personnel or the Network Administrator.

g. When you need to step away from your workstation or laptop, lock the screen or logout of the system.

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.** Network Administrator – The individual responsible for all LAN administrative duties in the College.
   - **b.** Protected – Personal, confidential, or otherwise sensitive information in electronic format or hard copy that is exclusively for the use of the owner and authorized entities.
8. **Revision History**
   - **a.** Policy is in effect on 01/01/2011
   - **b.** Document revised on 11/19/2010
     - b.i. Revised by Brett Ussher