

Smart Browsing Policy

1. Overview

- a. The purpose for this policy is to establish a set of guidelines to reduce the risks involved with using the Internet. Applying reason to Internet surfing will help prevent the unwanted infection of networked resources (e.g. desktop computers, laptops, etc.) as well as the time and inconvenience associated with correcting corrupted resources. All employees and students should familiarize themselves with the guidelines of this policy.

2. Purpose

- a. The main reasons for a smart browsing policy are:
 - i. Efficient and effective use of University assets.
 - ii. It reduces the threat of a security incident as visiting safe/trusted websites is less likely to result in infection.
 - iii. The integrity of protected information that might be located on infected systems (especially instructor or administrative systems).

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. When using the Internet or other networked resources.

5. Action

- a. **For Staff and Instructors:** Only visit websites and other networked resources that are related to your job.
- b. **For Instructors:** Additionally, resources related to proposed or ongoing research or course preparation (such as online tools for students) are permissible.
- c. **For Students:** Only visit websites that are related to schoolwork you are assigned to complete.
- d. Don't install or answer "Yes" or "Ok" to pop up windows without being completely certain of the resulting action. Ask your Network Administrator when in doubt of any pop-up windows. For students in one of the labs, you can ask either your instructor or the staff at the CLC Helpdesk.
- e. Keep the scope of your Internet usage to organizations that are well-known and have earned public trust to be free of malicious software (e.g. Google, Microsoft).
- f. Keep away from websites that consistently find themselves in the press for being infected with malicious software (e.g. Facebook, MySpace).
- g. When in doubt, ask yourself some questions:
 - i. Does this look like a reputable website? (Websites that look ad-hoc are more likely to contain questionable material or malicious software).
 - ii. Is this website trying to get me to install software?
 - iii. Is this website trying to redirect me to a website that I did not expect to be redirected to (or even know existed)?

- h. If a website does not appear to be safe, do what you must to leave the website without violating any of the above policy actions. Close the web browser if no other method can be found.
- i. Ensure when utilizing sites to transfer protected information (e.g. bank account numbers, credit card numbers, Social Security numbers), that SSL encryption is used and validated by a trusted CA.

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. CA – (Certificate Authority) An entity that issues digital certificates. The certificates are used by websites to prove the identity of the organization so that users know they are connected to the correct website and provide SSL encryption between the user's computer and the web server.
- b. CLC Helpdesk – (Common Learning Center) The staff that manage the CLC lab for the ISAT School.
- c. Network Administrator – The individual responsible for all LAN administrative duties in the College.
- d. 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.
- e. SSL – Encryption method used to keep network communications between two hosts on a network private. In regards to websites, the URL will use https (port 443) instead of http (port 80).

8. Revision History

- a. Policy is in effect on 01/01/2011
- b. Document revised on 11/19/2010
 - i. Revised by Brett Ussher