# Employee Internet Use Monitoring and Filtering Policy

***Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu***

**1.0 Purpose**
The purpose of this policy is to define standards for systems that monitor and limit web use from any host within <Company Name>'s network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

**2.0 Scope**
This policy applies to all <Company Name> employees, contractors, vendors and agents with a <Company Name>-owned or personally-owned computer or workstation connected to the <Company Name> network. This policy applies to all end user initiated communications between <Company Name>'s network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

**3.0 Policy**
**3.1 Web Site Monitoring**
The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

**3.2 Access to Web Site Monitoring Reports**
General trending and activity reports will be made available to any employee as needed upon request to the Information Technology Department. Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

**3.3 Internet Use Filtering System**
The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for <Company Name>'s corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing

- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

**3.4 Internet Use Filtering Rule Changes**
The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

**3.5 Internet Use Filtering Exceptions**
If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

**4.0 Enforcement**
The IT Security Officer will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**5.0 Definitions**
Internet Filtering – Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

User ID – User Name or other identifier used when an associate logs into the corporate network.

IP Address – Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

SMTP – Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.

Peer to Peer File Sharing – Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Social Networking Services – Internet sites such as Myspace and Facebook that allow users to post content, chat, and interact in online communities.

SPAM – Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Hacking – Sites that provide content about breaking or subverting computer security controls.

**6.0 Revision History**
11/23/2007 – Draft Completed, Kevin Bong