

<i>Jefferson County Policies & Procedures</i>			
Policy Name:	Employee Internet Use Monitoring and Filtering Policy	Approved:	11/7/2013
Policy Number:	101	Author:	Grim/Keyser
Associated:			

Purpose:

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the Jefferson County Commission’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. It is important that all employees understand that their computer, email, and Internet use are monitored and archived.

Policy:

Scope

This policy applies to all Jefferson County employees, contractors, vendors and agents with a County or official-owned or personally-owned computer or workstation connected to the Jefferson County Commission network.

This policy applies to all end user initiated communications between Jefferson County Commission’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.

Web Site Monitoring

The Information Technology Employees shall monitor Internet use from all computers and devices connected to the county 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 by the IT Department. Information disposition rules apply for the destruction of the records.

Access to Web Site Monitoring Reports

Department heads or Elected Officials can have access to reports, when requested. The county IT employees and authorized IT vendors 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 outside entities upon written or email request to the IT Department by the County Commission or Elected Officials.

Internet Use Filtering System

The county IT employees and authorized IT vendors shall block access to Internet websites and protocols that are deemed inappropriate for the county government environment. The following protocols and categories of websites shall be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging (outside of VOIP)
- 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

Internet Use Filtering Rule Changes

The network administrator shall periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

Internet Use Filtering Exceptions

If a site is not categorized properly, 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.

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 the network administrator. The network administrator will track approved exceptions and report on them upon request.

Enforcement

The network administrator will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. The network administrator will present any evidence of policy violation to the supervisor of the employee, and the County Administrator who will decide if/what disciplinary action may be appropriate.