11:02:03:00 Monitoring and Filtering Internet Use

Purpose:

The purpose of this policy is to define standards for systems that monitor and limit Internet use from any host within Dyersburg State Community College's (DSCC) network. These standards are designed to ensure employees and students use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

Scope:

This policy applies to all DSCC employees, students, contractors, vendors and agents using a DSCC-owned or personally-owned computer or workstation connected to the DSCC network. This policy also applies to all end-user initiated communications between DSCC's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

Policy:

Web Site Monitoring
The Information Technology Department shall reserve the right to monitor Internet use from all computers and devices connected to the corporate network. For example, monitoring may be done to investigate system problems or at the request of an employee's supervisor. The Vice President for Technology must be informed by the IT staff of any needed monitoring situation.

Access to Web Site Monitoring Reports
General trending and activity reports will be used as necessary for trouble-shooting and planning purposes. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the IT department upon written or email request to the Vice President for Technology.

Internet Use Filtering System
The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for DSCC's environment. The following protocols and categories of websites should be blocked:
• Adult/Sexually Explicit Material
• Advertisements & Pop-Ups

• Gambling
• Hacking
• Illegal Drugs
• Peer to Peer File Sharing
• Personals and Dating
• Spam, Phishing and Fraud
• Spyware
• Tasteless and Offensive Content
• Violence, Intolerance and Hate

Internet Use Filtering Rule Changes
The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules to the Vice President for Technology. Any 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 incorrectly categorized, employees may request the site be un-blocked by submitting a request to the Vice President for Technology. The Vice President for Technology will determine whether it should be unblocked.

Employees may access blocked sites with permission if appropriate and necessary for business or educational purposes.

Compliance:

The IT Staff may 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. Any student found to have violated this policy may be subject to disciplinary action, up to and including suspension.

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 (Internet Protocol 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 Breaking or subverting computer security controls.

Revision History:

Policy written April, 2011 by Vice President of Technology; approved by Administrative Council on 04/29/2011. Policy revised June, 2011; approved by Administrative Council on 06/21/2011.
