

M-04-26, Personal Use Policies and "File Sharing" Technology

M-04-26

September 8, 2004

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator, IT and E-Gov

SUBJECT: Personal Use Policies and "File Sharing" Technology

The purpose of this memorandum is to detail specific actions agencies must take to ensure the appropriate use of certain technologies used for file sharing across networks. These actions are based on recommended guidance developed by the CIO Council in 1999. The effective use and management of file sharing technology requires a clear policy, training of employees on the policy, and monitoring and enforcement.

Background

A type of file sharing known as Peer-to-Peer (P2P) refers to any software or system allowing individual users of the Internet to connect to each other and trade files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show, the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.

Federal computer systems or networks (as well as those operated by contractors on the government's behalf) must not be used for the downloading of illegal and/or unauthorized copyrighted content. It is important to ensure computer resources of the Federal government are not compromised and to demonstrate to the American public the importance of adopting ethical and responsible practices on the Internet.

The CIO Council has issued recommended guidance on "Limited Personal Use of Government Office Equipment Including Information Technology."¹ Examples of inappropriate personal use include "the creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited" and

"the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data."

Direction to Agencies

Effective use and management of file sharing technology requires a clear policy, training of employees on the policy, and monitoring and enforcement. Specifically, agencies are directed to:

1. **Establish or Update Agency Personal Use Policies to be Consistent with CIO Council Recommended Guidance.**

OMB expects all agencies to establish personal use policies, consistent with the recommended guidance developed by the CIO Council. Agencies who have not established personal use guidance should do so without delay, but no later than December 1, 2004.

2. **Train All Employees on Personal Use Policies and Improper Uses of File Sharing**

Agencies' IT security or ethics training must train employees on agency personal use policies and the prohibited improper uses of file sharing. Training must be consistent with OMB Circular A-130, appendix III paragraph (3)(a)(b) which states agencies must "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities [...]. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques."

On October 6, 2004, as part of the agency annual reports required by Federal Information Security Management Act of 2002 (FISMA) described in OMB Memorandum 04-25, FY 2004 Reporting Instructions for FISMA² agencies must report whether they provide training regarding the appropriate use of P2P file sharing.

3. **Implement Security Controls to Prevent and Detect Improper File Sharing**

As required by FISMA, agencies are to use existing NIST standards and guidance to complete system risk and impact assessments in developing security plans and authorizing systems for operation. Operational controls detailing procedures for handling and distributing information and management controls outlining rules of behavior for the user must ensure the proper controls are in place to prevent and detect improper file sharing.

Again, OMB recognizes there are appropriate uses of file sharing technologies, but as with all technology it must be appropriately managed.

If you have any questions regarding this memorandum, please contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail: jthornto@omb.eop.gov.