PEER-TO-PEER FILE SHARING 0933

(No.18 June 2005)

BACKGROUND

(No.18 June 2005)

This policy establishes the acceptable use of file sharing technologies such as Peer-to-Peer (P2P) File Sharing Programs. A Peer-To-Peer File Sharing Program is "computer software, or protocol, other than computer and network operating systems, that has as its primary function the capability to allow the computer on which the software is used to designate files available for transmission to another computer using the software, to transmit files directly to another computer using the software, and to request the transmission of files from another computer using the software." (State Administrative Manual, § 4840.4.) While P2P technology has many legitimate uses, these file-sharing programs are often used for the illegal dissemination and downloading of copyrighted material, including, but not limited to, music, motion pictures, software, and video games.

Using P2P, any computer can start or complete a file exchange with any other computer using the same program and connected over a shared network including the Internet. P2P applications like KaZaA, Gnutella, Blubster, eMule, Grokster, BitTorrent, Direct Connect and others are commonly used for the sharing of music and video files. P2P applications bypass many of the normal safeguards put in place for network security and the potential for copyright infringement is often overlooked. Inappropriate use of P2P and other technologies that allow network based sharing of files between computers also exposes information systems, data and information resources to risks, including virus attacks, and unauthorized disclosure of confidential or sensitive data and information. Traffic from the sharing of non-business related files over networks can also adversely affect network capacity needed for legitimate business transactions. In addition, this activity may also expose individuals as well as the Department to legal liability if the material being shared is copyrighted.

POLICY

This policy applies to all employees, consultants, contractors, or other non-CAL FIRE employees that are granted access to computing resources (hereby known as "employees") of the California Department of Forestry and Fire Protection. It is the responsibility of all California Department of Forestry and Fire Protection employees to know this policy and to conduct activities accordingly.

In order to comply with State policy, protect against computer viruses, prohibit illegal dissemination and downloading of copyrighted material by California Department of Forestry and Fire Protection employees, and ensure adequate Internet bandwidth for all users:

- Employees are not permitted to install or run P2P or any other file sharing program without prior consultation and written permission from the Chief Information Officer.
- P2P programs and other file sharing programs will only be allowed for legitimate State business. The use of such technology will be carefully monitored and controlled.
- All unauthorized P2P and other file sharing applications will be removed. If you have questions or concerns about the removal of an existing file sharing application, contact the Chief Information Officer within Information Technology Services.
- For security compliance and network maintenance purposes, authorized individuals within the California Department of Forestry and Fire Protection may monitor and/or audit equipment, systems, and network traffic at any time in accordance with all applicable statutes, regulations and State policies.
- The California Department of Forestry and Fire Protection reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- The California Department of Forestry and Fire Protection reserves the right to notify the employee in violation of this policy and/or his supervisor and may/will apply disciplinary action if warranted.

Authority

- ❑ State Administrative Manual (SAM) §4840.4 and 4841.2
- ❑ State of California Budget Letter 05-03
- ❑ Executive Order S-16-04

(see next section)

(see HB Table of Contents)

(see Forms or Forms Samples)