BUDGET LETTER

SUBJECT: PEER-TO-PEER FILE SHARING	**NUMBER:** 05-03
	DATE ISSUED: March 7, 2005
REFERENCES: STATE ADMINISTRATIVE MANUAL SECTIONS 4819.2, 4840.4, 4841.1, 4841.2, EXECUTIVE ORDER S-16-04	**SUPERSEDES:**

TO: Agency Secretaries
Department Directors
Departmental Budget Officers
Departmental Chief Information Officers
Departmental Information Security Officers
Department of Finance Budget Staff

FROM: DEPARTMENT OF FINANCE

Note: Budget Officers are requested to forward a copy of this Budget Letter (BL) to your department's Information Security Officers (ISOs) and department's Chief Information Officers (CIOs) even though the Finance State ISO Office will also distribute it separately to the ISOs and CIOs on the current contact list.

BACKGROUND

The Department of Finance (Finance) is responsible for establishing the framework for the state's information technology (IT) security policies and activities and for IT security oversight. This BL creates new policy regarding the practice of peer-to-peer file sharing to implement the Governor's Executive Order S-16-04.

When the word "agency" is used in the peer-to-peer policy and within this BL, the meaning is consistent with the definition in the State Administrative Manual (SAM) Section 4819.2: "When used lower case, (agency) refers to any office, department, board, bureau, commission or other organizational entity within state government."

POLICY

The following policy and definition are effective immediately. The changes will appear in the next revision of SAM. You may refer to Attachment I, "Advance Copy of Changes to SAM Sections 4840.4 and 4841.2" to see the context of this policy change.

Definition: **Peer-To-Peer File Sharing Program.** 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.

Policy: Each agency must establish a policy to ensure that the use of peer-to-peer technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property.

Business use of peer-to-peer technologies must be approved by the agency CIO and ISO.

The head of each agency is responsible for compliance with the policy described in this section. (See SAM Section 4841.1.)

DISCUSSION OF PEER-TO-PEER TECHNOLOGY

The technologies associated with peer-to-peer file sharing are varied and continuously evolving. While there are certain specific legitimate business applications for the use of peer-to-peer technologies for the state, it is acknowledged that this same technology is used for a variety of inappropriate or illegal uses such as exchange of copyrighted music. Hence, it is prudent for state organizations to institute reasonable measures to use peer-to-peer technologies appropriately and to prevent inappropriate uses.

An agency policy to restrict peer-to-peer file sharing will generally consist of multiple components, and the policy must be regularly reevaluated to ensure its continued effectiveness. In general, policies implemented to restrict peer-to-peer file sharing to legitimate business purposes will include at least some of the following components.

- Assessment to determine existing legitimate and authorized uses of peer-to-peer technology, if any, within an organization.
- Configuration of existing operating system, network, and security and application systems to block or restrict unauthorized peer-to-peer activities.
- Implementation of special-purpose software and hardware products designed to control the use of peer-to-peer technology.
- Controlling the installation and use of peer-to-peer software and other unauthorized software on workstations and servers.
- Educating staff and contractors on state and department policy regarding peer-to-peer technology.
- Careful evaluation, implementation and monitoring of legitimate peer-to-peer applications and systems to ensure that they do not enable illegitimate uses of those capabilities.
- Regular testing and monitoring activities to ensure that the peer-to-peer restrictions continue to operate effectively.

Legitimate use of peer-to-peer technology is typically limited to:

- A technical data transfer component built into some business applications.
- A process used by authorized technical staff to transfer business data from one server or mainframe computer to another.

Precautions for those departments that use peer-to-peer technology:

- Know who is using it and for what purpose.
- Monitor the approved uses for adherence to policy and standards.
- Watch for evidence of unauthorized use, including:
    - unusual network traffic
    - traffic on ports that your department does not typically use
    - presence of unauthorized software
    - presence of large and unauthorized files on servers and desktops
- If unauthorized peer-to-peer activity is detected, take immediate action to stop the activity and perform necessary system checks. Watch for configuration problems, illegal/unapproved software and intellectual property, spyware, and worms and viruses.

CONTACTS AND QUESTIONS

You may call the State ISO Office at (916) 445-5239 if you have questions about this BL.

/s/ Greg Rogers

Greg Rogers
Assistant Program Budget Manager

Attachment

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

New text is in italics; nothing was deleted.

4840.4 DEFINITIONS

Confidential Information. Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws. See SAM Section 4841.3.

Critical Application. An application that is so important to the agency that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or on the continuation of essential agency programs.

Custodian of Information. An employee or organizational unit (such as a data center or information processing facility) acting as a caretaker or an automated file or data base.

Disaster. A condition in which an information asset is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Hardening. A defense strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.

Information Assets. (1) All categories of automated information, including (but not limited to) records, files, and data bases; and (2) information technology facilities, equipment (including personal computer systems), and software owned or leased by state agencies.

Information Integrity. The condition in which information or programs are preserved for their intended purpose; including the accuracy and completeness of information systems and the data maintained within those systems.

Information Security. The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Owner of Information. An organizational unit having responsibility for making classification and control decisions regarding an automated file or data base.

Peer-To-Peer File Sharing Program. *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.*

Physical Security. The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

Privacy. The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Public Information. Any information prepared, owned, used, or retained by a state agency and not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Risk. The likelihood or probability that a loss of information assets or breach of security will occur.

Risk Analysis. The process of evaluating: (a) the vulnerability of information assets to various threats, (b) the costs or impact of potential losses, and (c) the alternative means of removing or limiting risks.

Risk Management. The process of taking actions to avoid risk or reduce risk to acceptable levels.

Sensitive Information. Information maintained by state agencies that requires special precautions to protect it from unauthorized modification, or deletion. See SAM Section 4841.3. Sensitive information may be either public or confidential (as defined above).

User of Information. An individual having specific limited authority from the owner of information to view, change, add to, disseminate or delete such information.

4841.2 INFORMATION INTEGRITY AND SECURITY

Each agency must provide for the integrity and security of its information assets by:
Identifying all automated files and data bases for which the agency has ownership responsibility (see SAM Section 4841.4);

Ensuring that responsibility for each automated file or data base is defined with respect to:

a. The designated owner of the information within the agency,

b. Custodians of information, and

c. Users of the information;

d. Ensuring that each automated file or database is identified as to its information class (SAM Section 4841.3) in accordance with law and administrative policy;

e. Establishing appropriate policies and procedures for preserving the integrity and security of each automated file or data base including:

    1. Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information and information necessary for the support of agency critical applications;

    2. Periodically changing dial-up access telephone numbers, and

3. Responding to losses, misuse, or improper dissemination of information.

2. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:

   a. Technology upgrade policy, which includes, but is not limited to, operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.

   b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, and firewalls. The policy must address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.

   c. Firewall configuration policy, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

   d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

   e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy must address, and be consistent with, the department's policy for making security upgrades and security patches.

   f. Policy to ensure that the practice of peer-to-peer file sharing for any use not related to state business is prohibited and does not take place within the agency. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property. Business use of peer-to-peer file sharing programs must be approved by the agency CIO and ISO.

The head of each agency is responsible for compliance with the policy described in this section. (See SAM Section 4841.1.)

Each state data center must carry out these responsibilities for those automated files and databases for which it has ownership responsibility. See SAM Sections 4841.4 and 4841.5.

Oversight responsibility at the agency level for ensuring the integrity and security of information assets, including automated files and databases, must be vested in the agency Information Security Officer.