Office of Systems Integration "SERVING CALIFORNIA"	**Security Policy** **Control Number: OSI-SP-08-08**
Acceptable Use Security Policy	**Effective Date: May 22, 2008**

Purpose

Information resources are strategic assets of the Office of Systems Integration (OSI) and must be treated and managed as valuable resources. OSI provides various computer resources to its employees for the purpose of assisting them in the performance of their job-related duties. State law permits minimal and incidental access to state resources for personal use. This policy clearly documents expectations for appropriate use of OSI assets. The Acceptable Use Security Policy, in conjunction with the corresponding standards, is established to achieve the following:

1. To establish appropriate and acceptable practices regarding the use of information resources.
2. To ensure compliance with applicable state law and other rules and regulations regarding the management of information resources.
3. To educate employees with respect to their responsibilities who may use state government resources.

Scope

This policy applies to all OSI full-time or part-time employees, contractors who are authorized to use state government-owned or leased equipment or facilities, and volunteers who are authorized to use and have been provided with access to state government resources. All users are required to read the policy and must sign the OSI Acceptable Use Security Policy Acknowledgement Form.

Policy

Acceptable Use Management Requirements

OSI will establish formal standards and processes to support the ongoing development and maintenance of the OSI Acceptable Use Security Policy.

The OSI Director and management will commit to the ongoing training and education of OSI staff responsible for the administration and/or maintenance and/or use of OSI

Policy (continued)

information resources. At a minimum, skills to be included or advanced include security awareness training.

1. The OSI Information Security Office may create supporting documentation to amplify the intent of this policy and to address requirements from governing entities or documents.
2. The OSI Information Security Office will establish a formal review cycle for all acceptable use initiatives.
3. Any security issues discovered will be reported to the Information Security Officer (ISO), or designee, for follow-up investigation (OsiInfosecurityoffice@osi.ca.gov). Additional reporting requirements can be located within the Acceptable Use Requirements section of this policy.

Ownership

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of OSI are the property of OSI and employee use of these files is neither personal nor private. Authorized OSI information security employees may access such files at any time without knowledge of the information resource's user or owner. OSI management reserves the right to monitor and/or log all employee use of OSI information resources with or without prior notice. Users of OSI and state resources shall have no expectation of privacy in the use of these resources.

Acceptable Use Requirements

1. Users must report any weaknesses in OSI computer security to the appropriate security staff. Weaknesses in computer security include, but are not limited to, unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
2. Users must report any incidents of possible misuse or violation of this Acceptable Use Security Policy through the use of the OSI Information Security Incident Response Policy.
3. Users must not attempt to access any data, documents, email correspondence, and programs contained on OSI systems for which they do not have authorization.
4. Systems administrators and authorized users must not divulge remote connection modem telephone numbers or other access points to OSI computer resources to anyone without proper authorization.
5. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), security tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes.
6. Users must not make unauthorized copies of copyrighted or OSI owned software.

Acceptable Use Requirements (continued)

7. Users must not use non-standard shareware or freeware software without the appropriate OSI management approval.
8. Users must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material which OSI may deem to be offensive, indecent or obscene.
9. Users must not purposely engage in activity that is illegal according to local, state or federal law.
10. Users must not engage in activity that may degrade the performance of information resources; deprive an authorized user access to OSI resources; obtain extra resources beyond those allocated; or circumvent OSI computer security measures.
11. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of an OSI computer resource unless approved by the OSI's Information Security Office.
12. OSI information resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
13. Access to the Internet from OSI owned or leased, home based, computers must adhere to all pertinent policies. Employees must not allow family members or other non-employees to access nonpublic accessible OSI computer systems.
14. Any security issues discovered will be reported to the ISO, or designee, for follow-up investigation. Additional reporting requirements can be located within the Information Security Incident Response Policy.

The OSI Acceptable Use Security Policy does not supersede state and federal laws and guidelines.

Minimal and Incidental Use

Government Code Section 8314 permits minimal and incidental personal use of state resources. At OSI this means:

1. Minimal and incidental personal use of electronic mail, Internet access, fax machines, printers, phones, and copiers is restricted to OSI approved users only and does not include family members or others not affiliated with OSI.
2. Minimal and incidental use must not result in direct costs to OSI, cause legal action against, or cause embarrassment to OSI.
3. Minimal and incidental use must not interfere with the normal performance of an employee's work duties.

Minimal and Incidental Use (continued)

4. Storage of personal electronic mail messages, voice messages, files and documents within OSI's computer resources must be minimal.

OSI management will resolve minimal and incidental use questions and issues in collaboration with the OSI's ISO, Human Resources Manager and Legal Counsel.

Roles and Responsibilities

1. OSI management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.
2. OSI management is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under the Exceptions section.
3. OSI Managers, in cooperation with the Information Security Office, are required to train employees on the Acceptable Use Security Policy and document issues with policy compliance.
4. All OSI employees are required to read and acknowledge the reading and understanding of this policy.

References

Government Code Section 8314

OSI Information Security Incident Response Policy OSI-ITS-07-01

OSI Encryption on Portable Computing Devices Policy OSI-AP-06-09

OSI Password Standard OSI-AP-07-03

Disclaimer

Access to Internet services is made available by OSI to users as a privilege. The Internet has the ability to provide access to sites and information which is not under the control of OSI. OSI makes no representation concerning the content of these sites nor should the fact that the employer has provided access be construed or interpreted as an endorsement by OSI. Information found on the Internet does not represent an official record of OSI. OSI makes no warranty as to the accuracy, reliability, completeness or timeliness of any information provided on the Internet and are not responsible for any errors, omissions or for results obtained from the use or misuse of information found on the Internet.

Liability

Users of electronic mail and the Internet accept responsibility for any and all actions, and consequences of said actions, while using the electronic mail and the Internet. OSI accepts no responsibility for any actions taken by electronic mail and Internet users.

Exceptions

Exceptions to this policy will be considered only when the requested exception is documented and presented to the OSI Information Security Office.

Violations/Enforcement

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of OSI information resources access privileges, civil, and criminal prosecution.
2. The OSI Information Security Office is responsible for the periodic auditing and reporting of compliance with this policy. The OSI Information Security Office will be responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to OSI management.

Approval

ORIGINAL SIGNED BY PAUL BENEDETTO **5/23/08**

PAUL BENEDETTO Date
Chief Deputy

ACCEPTABLE USE SECURITY POLICY

SECURITY RESPONSIBILITIES AND ACKNOWLEDGEMENT

The Office of Systems Integration (OSI) makes its computing resources available to employees, authorized contractors, and volunteers as a necessary tool. The OSI computing resources, such as the Internet, are provided to employees, authorized contractors, and volunteers for the purpose of conducting OSI-approved activities. All users are responsible for using these resources in an effective, ethical, and lawful manner. The OSI prohibits unauthorized access, disclosure, duplication, modification, diversion, loss, misuse, or theft of information assets either owned by, or entrusted to, the OSI. As a condition of using the OSI computing resources, every user is required to understand and comply with the Acceptable Use Security Policy and all relevant laws, regulations, policies and practices governing the use of state-owned computing resources.

ACKNOWLEDGEMENT

I have read the OSI Acceptable Use Security Policy and have read and understand the above policy statement. I understand that my failure to adhere to the OSI computing policy could result in my being denied access to information and computing resources, and could be grounds for adverse action, up to and including termination.

Additionally, I understand that all computing activities conducted on OSI systems are subject to monitoring and that OSI reserves the right to monitor and log all computing activities, including the use of the Internet, with or without notice. I understand that the computing resources are the property of OSI and I have no expectation of privacy when using these resources.

I understand this signed acknowledgment form shall be kept in my official personnel file.

Employee's Name (Printed)	Employee's Office
Employee's Work Telephone Number	Employee's Work Address

Employee's Signature	Date