# STATEWIDE INTERNET USAGE POLICY

*The Department of Information Technology*

## POLICY STATEMENT

Each agency shall define and implement an acceptable Internet use policy for its employees to facilitate the efficient and productive use of the Internet as a means to accomplish the agency's mission and program goals. Agency policies shall meet minimum requirements as stated in Section 1 of this policy statement.

Each state agency that will provide, exchange and access information via the Internet and/or the World Wide Web needs to plan and implement these services by establishing necessary procedures to ensure the security of state data resources and to facilitate the efficient and productive use of those resources. Guidelines for agency planning are provided in Section 2 of this policy statement.

## PURPOSE

To define the acceptable and unacceptable uses of the Internet by state employees in the performance of their duties and to help agencies plan for Internet usage when it is the most cost effective and technologically efficient vehicle for the dissemination and exchange of information.

## OVERVIEW

The Internet is one of many efficient and timely communication tools that can be used by state employees to accomplish government functions and to conduct the state's business within its organization, with other governmental agencies, and with the public. The Internet can also be used to publish the agency's mission, function, structure, goals, authority, address, phone numbers, information required by law or executive order; and other information of general interest to the public. As with any state-provided resource, the use of this resource should be limited to legitimate state business and is governed by rules of conduct similar to those applicable to the use of other information technology resources.

## OBJECTIVES

- Establish minimum requirements for state agency Internet policies.
- Establish guidelines for delegation of responsibility within. state agencies for defining the acceptable and unacceptable Internet uses for agency employees including procedures for them to access and post information in the most cost effective and technically efficient manner.
- Establish guidelines for assessing and addressing issues concerning secure access to the Internet and provide guidance in developing and implementing agency enforcement policies.
- Establish guidelines for delegation of responsibility within state agencies for maintaining, updating, and correcting information provided over the Internet.

## RESPONSIBILITIES

The following are responsible for implementing this policy:

- *DOlT Management* - to set policies and suggest guidelines for state agency Internet policy content to promote consistent statewide Internet usage.

- *Agency Management* - to develop agency Internet policies, set procedures for accessing the Internet, and set procedures for dealing with misuse of ~e Internet. These policies and procedures can be developed as stand-alone documents or be combined with other agency policies.

- *Internet User* - to follow all agency Internet policies and procedures.

**EVIDENCE OF COMPLIANCE**

To demonstrate compliance with this policy, the following documentation must be available:

- Agency Internet Policy Statement

- Signed User Consent Forms or User Sign-On Screens

- Agency Policies and Procedures

# SECTION 1: INTERNET USAGE POLICY REQUIREMENTS

**PURPOSE AND SCOPE**

The DOIT encourages state organizations to use the Internet as an integral part of its overall IT processes provided that they establish policies directing the appropriate use of the Internet. Use of the Internet is encouraged to:

- Provide an efficient method to exchange information within state agencies, between governmental agencies, and to the public.

- Facilitate the implementation of statewide e-mail systems.

- Provide sources of data to assist state organizations in accomplishing their stated mission and program goals.

It is also a responsibility of the DOIT to ensure that state organizations control information provided via the Internet or accessed by state employees over the Internet in a disciplined, managed, and consistent manner and that each organization publish their policy and established procedures once they are developed. In addition to adhering to the following policies and restrictions, the DOIT suggests that all state employees use the following test to determine if their use of the Internet is necessary of appropriate: Each employee should ask the question, "Is my use of the Internet enabling me to perform my duties more effectively, less expensively, or to provide better service to the taxpayers?" If the answer is not "yes," then the employee's Internet usage is either unnecessary or inappropriate.

The following information included in Section I is intended to support the DOITs policy statement and includes the following: Common terminology, minimum requirements for agency policies, a sample consent form, and suggested questions for agency management to consider as they develop their Internet policy.

**TERMINOLOGY**

Provided below are definitions and common terms used in discussing the Internet:

Confidential Information: Confidential information is that which is protected under the California Public Records Act [CAL. Gov't. Code 6250-6270 (West 1996)].

E-mail: Electronic mail is a means of sending messages between computers using a computer network or over a modem connected to a telephone line.

Internet: The Internet is a medium through which information or electronic mail may travel. Computer users can currently use the Internet like a telephone or fax to exchange information quickly and efficiently.

Client: One end of a network protocol that provides a user interface to the server end.

Server: Computers that provide information to client programs via the Internet through programs that send information to Web browsers such as Netscape Navigator and Microsoft Internet Explorer.

Server: Computers that provide information to client programs via the Internet through programs that send information to Web browsers such as Netscape Navigator and Microsoft Internet Explorer.

Computing Ethics: A set of accepted manners to be observed while using the Internet.

World Wide Web (WWW or the Web): This is the part of the Internet which provides a way for organizations or individuals to publish information which is then available to a world-wide audience. Currently, the World Wide Web uses an Internet protocol called HTTP or HyperText Transfer Protocol and sends files written in a language called HTML or HyperText Markup Language - an HTTP server provides Web pages to client programs called browsers which retrieve and display the information stored on the Web server.

Home Page: This is a starting point for most organizations to place links to other parts of the Web; for example, the state of California could have its own home page which is linked to various branches of government, the Legislature, the Judiciary; and the Executive branch.

Web Page: A single page displayed by a Web browser.

## MINIMUM INTERNET USAGE POLICY REQUIREMENTS

The information included in this section serves as the minimum requirements for a state organization's Internet policy. The DOIT encourages the addition and augmentation of information to each agency's policy which covers material unique to the entity's environment and user population. These policy statements can exist as a stand-alone policy or can be incorporated into other agency IT policies. These minimum requirements may need to be slightly altered; however, the actual meaning should not be changed without approval of the State CIO.

### INFORMATION CONTENT AND USE OF THE SYSTEM - ACCEPTABLE USES

**The state reserves the right to monitor and/or log all network activity with or without notice, including e-mail and all web site communications, and therefore, users should have no reasonable expectation of privacy in the use of these resources.**

*Uses that are acceptable and encouraged:*

- Communications and information exchanges directly relating to the mission, charter, and work tasks of the agency;
- Announcements of state laws, procedures, hearings, policies, services, or activities;
- Use for advisory, standards, research, analysis, and professional society or development activities related to the user's state governmental duties; and
- Use in applying for or administering grants or contracts for state government research programs.

*Uses that are unacceptable:*

It is unacceptable for a user to use, submit, publish, display, or transmit on the network or on any computer system any information which:

- Violates or infringes on the rights of any other person, including the right to privacy;
- Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- Violates agency or departmental regulations prohibiting sexual harassment;

- Restricts or inhibits other users from using the system or the efficiency of the computer systems;
- Encourages the use of controlled substances or uses the system for the purpose of criminal intent; or
- Uses the system for any other illegal purpose.

*It is also unacceptable for a user to use the facilities and capabilities of the system to:*

- Conduct any non-approved business;
- Solicit the performance of any activity that is prohibited by law;
- Transmit material, information, or software in violation of any local, state or federal law;
- Conduct any political activity;
- Conduct any non-governmental-related fund raising or public relations activities;
- Engage in any activity for personal gain or personal business transactions; or
- Make any unauthorized purchases.

**COPYRIGHTED MATERIAL**

Users may download copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law. The federal Copyright Act at 17 U.S.C. 101 *et. seq.* (1988), protects and prohibits misuse of all original works of authorship in any tangible medium of expression. This includes a prohibition on plagiarism (using someone else's ideas or writing ~ passing it on as one's own).

**PUBLIC DPMAIN MATERIAL**

Any user may download public domain programs for his/her own business-related use, or may redistribute a public domain program non-commercially but does so with the knowledge that by doing so, he/she also assumes all of the risks regarding the determination of whether or not a program is in the public domain~

**ELECTRONIC MAIL [E-MAIL]**

E-mail is considered network activity, thus, it is subject to all policies regarding acceptable/unacceptable uses of the Internet and the user should not consider e-mail to be either private or secure.

**REGULATION AND ENFORCEMENT**

Agency secretaries and independent directors (or their delegated representatives) are responsible for compliance with provisions of this policy and for investigating suspected non-compliance. These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of the policy; and
- Suspension of service to users or of user access with or without notice when deemed necessary for the operation and/or integrity of the state communications infrastructure or connected networks.

When an instance of non-compliance is suspected or discovered in a computing system or network connected to the state network, the agency shall proceed in accordance with agency and Civil Service rules. Internal discipline, up to and including discharge, may be appropriate in some cases of non-compliance with this policy. Criminal or civil action may be initiated in appropriate instances.

**CONSENT FORM**

All state employees having access to the Internet must consent that all network activity is the property of the state, and therefore, they should not consider any activity to be private. This should be accomplished through a signed Consent Form. (shown below as Figure 1-1). The method to obtain and maintain these forms should be included in the agency's policy.

This following is a sample of text that might appear on a consent form. As a minimum, anyone having access to the Internet must acknowledge that they are consenting to the state's having possession of and access to all network activity.

FIGURE 1-1

SAMPLE CONSENT FORM

I________________have read this policy and agree to comply with all its terms and conditions. I agree that all network activity conducted while doing state business and being conducted with state resources is the property of the State of California.

The state reserves the right to monitor and log. all network activity including e-mail, with or without notice, and therefore users should have no expectations of privacy in the use of these resources.

Signed______________________________________

Date:_______________________________________

Supervisor___________________________________

Date:_______________________________________

LIABILITY

This state agency makes no warranties of any kind, whether expressed or implied, for the service that is the subject of this policy. In addition, state agencies will not be responsible for any damages whatsoever which employees may suffer arising from or related to their use of any state agency electronic information resources, whether such damages be incidental, consequential or otherwise, or whether such damages include loss of data resulting from delays, non-deliveries, mistaken deliveries, or service interruptions whether caused by either a state agency's negligence, errors, or omissions. Users must recognize that the use of state agency electronic information resources is a privilege and that the policies implementing usage. are requirements that mandate adherence.

DEVELOPING AN AGENCY POLICY AS PART OF THE OVERALL AGENCY IT STRATEGY

The following questions are suggested to assist in the development of an agency's Internet policy. Agencies should develop their policies in coordination with their overall IT strategies and address, at a minimum, the following issues:

*Internet Access*

- Who needs access to the Internet and why?
- Should there be certain criteria for determining who really needs Internet access?
- Should Internet access be automatically available to anyone on a department LAN?
- What type of Internet access will be allowed?
- What restrictions should there be?

- How is access limited to business usage?
- How should the use of the Internet be monitored?
- What will be the consequences of misuse or abuse of Internet access?
- How does Internet access relate to the agency/working group computing policy?

*Providing Public Info7712ation*

- Who will be responsible for determining the appropriate information and what will be the approval process for providing information to the public [the California Public Records Act will be applicable to this material]?
- Who will have preparation responsibility for information publicly disseminated?
- Who will be responsible for keeping information current and accurate?
- Who will establish home pages and will there be restrictions on establishing these home pages?

*Use of Internet for E-mail*

- What will be our need for policies of appropriate Internet e-mail usage?
- Can our Internet e-mail policy be consistent with or combined with our department e-mail policy?

*Acquiring Info7712ation via the Internet*

- What will the process be to acquire information via the Internet?
- How will usage of the Internet be limited to support business goals?
- What will be the process/policy for prohibiting the downloading of proprietary software?
- What other accessible information will be restricted?
- Who will determine access restrictions?
- Should there be restrictions on the size of downloaded files, and if so, who will establish these restrictions?

*Accessing the Internet*

- What is the most cost effective and secure way to provide Internet access?
- Should there be a department-wide standard for the technical means to access the Internet, i.e., for software, security measures, moderns, or network connections?
- How will IT resources supporting Internet usage be managed including but not limited to those resources used for other IT functions?
- What functional unit will be responsible for technical support of accessing and using the Internet and will that unit also be responsible for supporting the home page and related links?

*Security Issues*

- 'What will be the Information Security Officer's [ISO's] role in developing, maintaining, and monitoring Internet access security policies?
- 'What are the security risks?
- How will security compromises best be prevented?
- How will confidentiality be maintained where required?
- 'Who will determine and what will be the consequences for failing to follow security rules?

*Accountability and Fiscal Responsibility*

- 'What will be the standards for proper usage and professional behavior?
- 'What are the legal consequences, if any, to be considered?
- How will the costs associated with Internet access be allocated?

*Update and Dissemination of Internet Policy*

- Should the Internet policy be included in the department's operations manual?
- How often should the policies be reviewed for currency and accuracy given the rate at which technology becomes obsolete?

# SECTION 2: GUIDELINES FOR PLANNING AND IMPLEMENTING AGENCY INTERNET POLICY

## INTRODUCTION

The information provided in Section 2 is intended to assist agencies in developing Internet planning and implementation procedures. State organizations are encouraged to share additional information to continually improve this process. This section includes discussion of connection to the Internet, support services, security, distribution of information, and general planning concerns.

## INTERNET PLANNING

All topics discussed as part of this section require the agency to develop a plan and strategy for the Internet. The use of the Internet should be part of the state organization's strategic and tactical plans~ The actual connections, security systems, and Internet software should be part of the organization's network configurations lists and drawings.

## BASICS OF PROVIDING INTERNET ACCESS

As with the use of other IT capabilities, each state organization will need to decide how to provide Internet access and what this access will accomplish. Two options for connection are contracting with a private Internet Service Provider or contracting with a state data center that serves as an Internet Service Provider.

## INTERNET CONNECTION AND SOFTWARE

In cases where the connection will be acquired outside the organization, an Internet account is needed. The Internet Service Providr then makes the actual connection to the organization's IT infrastructure and to the Internet backbone. The agency must choose a w, to connect to the Internet Service Provider; for example, by modem or by connecting the communication devices to an organization Local Area Network, or both. The Internet Service Provider can help in selecting the necessary communication devices and provide help in installing equipment, phone lines, etc.

Connection to the Internet also requires the use of software systems which should be chosen by the appropriate agency/department official in coordination with the agency's overall IT program. There are many software tools that have been established to assist in connecting to the Internet, developing home pages, browsing (searching) the Internet sites, and with general utilities. As with other software, each state organization should define a standard software system(s) to accomplish the basics and define a user support process. Both of these definitions should be instituted in written procedures and processes that have assigned staff responsible for maintaining each. Organizations should also consider the benefits of browsing other Internet sites and posted home sites, and of establishing an agency or department home page to distribute and/or collect information relative to the organization's business-related products.

## HOME PAGE

The use of home pages by both public and private entities has been rapidly expanding. At first home pages served as advertisements displaying relatively static information. Home pages have evolved into interactive tools used to both distribute and collect information directly into the organization's database systems. State organizations need to give careful consideration to how they will use a home page, how they will develop their home page, how they will maintain their home page over time, and how they will coordinate their home page with the state home page which is operated by the state library.

If an agency decides to use a home page, it should contain the agency's seal, information about the agency including its mission statement, and information on how to contact the agency bye-mail, by regular mail, or by telephone. The following issues should be considered in setting up a home page:

- Presentation of additional information specific to each agency should be carefully planned in. accordance with other DOIT policies and with the agency's overall IT plan.
- Home pages reflect the image and reputation of an agency; thus, it is important to establish an on-going process for updating the content, appearance, and usability of all information that appears and that is supplied to the public.
- Confidential information shall not be released to the public via the Internet.
- Release of information that would compromise public safety should always be avoided.
- If an agency intends to provide public access to information over the Internet, a procedure should be established for what kinds of documents and information are going to be provided and how both incoming and outgoing information will be received and supplied.

## SECURITY

An important function of Internet planning and implementation is to make users aware of the potential security threats of exchanging, sending, and receiving information over the Internet. As with other IT assets, care and planning should be taken to ensure a "safe computing environment." This should include processes:

- To report known security weaknesses and breaches.
- To prevent security weakness exploitation by hackers.
- To employ, when appropriate, any security measures using software and/or hardware configurations that will protect the network or ensure that sensitive communications are transmitted securely over the insecure Internet network.

- To utilize updated network security information and resources to protect network integrity and security.
- To develop policies to enforce proper distribution of agency information and prevent the distribution, whether inadvertent or intentional, of restricted or proprietary information.
- To develop policies to protect against virus attacks by reminding employees of the risk of downloading information from unknown sources on the Internet (note also that not all viruses can be detected by virus scanning programs).
- To develop policies on using aliases for communications over the Internet.
- To develop policies to deal with financial transactions over the Internet. While few agencies conduct financial transactions over the Internet, this may become a more widely used service in the future. When considering offering such services, a security procedure to protect the privacy of the credit-card payments or any other payment must be established by the agency. Agencies planning financial transactions over the Internet also need to consider how they will maintain security while electronically transacting with financial institutions, other agencies, or the public. Agencies also must consider requirements of the Internal Revenue Service regarding computerized business.
- To develop policies for user support, employee training, and system maintenance.
- To develop policies to prevent the release of information that may misrepresent the agency's positions, that may be sensitive or unauthorized, or that may be unfinished and not ready for dissemination. .
- To develop policies to alert users to potential violations of Federal Trade Commission Rules or federal laws.

## COMPUTER ETHICS

As a representative of the State of California, state employees have a responsibility to conduct themselves in an ethical manner.

The following information suggests some areas where ethics issues will arise and provides some suggestions for issues that may need to be addressed in an agency policy:

- Data obtained inappropriately should not be used.
- Finding and reporting a system weakness is not a license to take advantage of it.
- Every user has a responsibility to do good work and to be accountable for that work.
- Organizations and individuals have rights to privacy.
- When the confidentiality of information is unclear, it should not be divulged.
- Electronic mail should be treated as privileged in the same manner as first class U.S. mail.
- Use of personal information voluntarily provided, for purposes other than agreed to, is unethical.

### ETIQUETTE ON THE INTERNET

It is essential that users recognize the each network/system has its own set of policies and procedures. Actions which are routinely allowed on one network/system may be controlled or even forbidden on other networks. It is the user's responsibility to abide by the policies and procedures of all networks/systems with which they may communicate.

The agency should develop etiquette policies covering user conduct including, but not limited to the following:

- The length and subject matter of messages;
- Proper presentation of messages (I.e., capitalizing, using asterisks, etc.);
- Prohibitions on commercial activity;
- Copyright laws and license/contract agreements on material usage; and
- Prohibitions or access limits for use of Internet mailing 11515, discussion groups, news groups, listservers, or any other interactive communication vehicle on the Internet.

## COMPUTER LAW AND COMPUTER CRIME

As the use of automated systems has grown, so too has the number of laws impacting the use of these automated systems. Agencies should develop ways to let Internet users know that virtually every state has laws covering abuse of computer communications and data transmissions that may apply to their Internet use.

Additionally, there are at least two federal laws, the Computer Fraud and Abuse Act of 1986 and the Electronic Communications Privacy Act of 1986, which have been enacted to control abuses of computers and electronic communications/data transmissions. In California, Section S020f the Penal Code prohibits tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. This law includes criminal penalties for introducing contaminants (viruses and worms) into computer systems and networks, allows the court to seize the hardware and software used in the commission of a computer crime, and allows the courts to consider prohibiting persons convicted of computer crimes from ever having access to computers in employment. Users should be made aware of these statutes and any other laws that the agency so chooses to best prevent misuse of the Internet-and best ensure protection of both the integrity and security of the state's network and systems.