

Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P1000 GENERAL POLICIES

Category: P1050 – EMPLOYEE INTERNET USE, MONITORING AND FILTERING

CONTENTS:

- I. [Authority](#)
- II. [Abstract](#)
- III. [Definitions](#)
- IV. [Policy](#)
- V. [Exemption Process](#)
- VI. [Procedure Reference](#)
- VII. [Contact Information](#)
- VIII. [Responsibilities](#)
[Revision History](#)

I. AUTHORITY

Authority: Idaho Code § 67-5745C(3)
Executive Order 2005-22

Idaho statute states in part “the Idaho Technology Authority shall:

Within the context of its strategic plans, establish statewide information technology and telecommunications policies, standards, guidelines, conventions and comprehensive risk assessment criteria that will assure uniformity and compatibility of such systems within state agencies;”

II. ABSTRACT

This Employee Internet Use Monitoring and Filtering policy is designed to help employees understand management’s expectations for granting employees access to the Internet and to help employees to use State resources wisely. While a direct connection to the Internet offers a variety of benefits to the State of Idaho, it can also expose the State to significant risks of its data and systems if appropriate security measures are not employed. Excessive, unnecessary Internet usage causes network and server congestion and reduces employee productivity. Unlawful Internet usage may also expose the State of Idaho and/or the individual user to legal liability.

III. DEFINITIONS

1. Internet – The Internet is a network of connected sites accessible through a “web browser” and is a resource for research, information gathering, extending and obtaining services, and education.

3. Worm – A malicious computer program that replicates itself over a computer network and usually performs unwanted actions, such as monopolizing the computer or network’s resources and shutting systems down.
4. Virus – A program or piece of code that is loaded onto a computer without the user’s knowledge and runs against the user’s wishes. It may contain a self-replicating component to spread the “infection” and almost always corrupt or modify files on a targeted computer.
5. Trojan Horse – A destructive program that masquerades as a benign application. Unlike viruses, Trojan Horses do not replicate themselves but they can be as destructive. They are typically used by cybercriminals for online fraud and theft.

IV. POLICY

A. Internet Monitoring

Each agency shall ensure that Internet use from all computers and devices connected to the state network are monitored. Records of the monitored traffic should be retained based on agency requirements.

B. Internet Filtering

Each agency shall ensure that access to websites and protocols that are deemed inappropriate (e.g. the criteria in Section C, sub-section 6, A thru M) is blocked.

C. Internet Use

1. Access to the Internet is a tool for meeting the business needs of the agency. Internet access is considered State property and the agency has the right to monitor the use of such property at any time. Therefore, users should not have any expectation of privacy as to their Internet usage via State computers and networks
2. The primary purpose of Internet use is to conduct official business. Employees may occasionally use the Internet for individual, nonpolitical purposes on their personal time, if such use does not violate the terms and conditions of this policy or interfere with State business.
3. Users may not download, store, transmit, or display any kind of image or document on any department system that violates federal, state, or local laws and regulations, Executive Orders, or that violate any ITA or department adopted policies, procedures, standards, or guidelines.
4. Users may not attempt to access prohibited content or to circumvent software put in place by the agency to prevent such access.

5. If a user accidentally connects to a site that contains sexually explicit or otherwise offensive material, he/she must disconnect from that site immediately and report the incident to their supervisor.
6. Use of the Internet as described below is **strictly prohibited**:
 - A. Viewing or distributing obscene, pornographic, profane, or sexually oriented material;
 - B. Violating laws, rules and regulations prohibiting sexual harassment;
 - C. Encouraging the use of controlled substances for criminal or illegal purposes;
 - D. Engaging in any activities for personal gain;
 - E. Obtaining or distributing copyrighted information without permission;
 - F. Obtaining and distributing advertisements for commercial enterprises, including but not limited to, goods, services, or property;
 - G. Violating or infringing upon the rights of others;
 - H. Conducting business unauthorized by the department;
 - I. Obtaining or distributing incendiary statements, which might incite violence or describe or promote the use of weapons;
 - J. Obtaining or exchanging proprietary information, trade secrets, or any other privileged, confidential, or sensitive information that is not authorized;
 - K. Engaging in any political activity prohibited by law;
 - L. Using the system for any illegal purpose; and
 - M. Accessing sites that are known to distribute malware software that is intended to damage disrupt or gain access to state resources.
7. Users may access any State owned web site for the purpose of conducting State authorized business, such as the online payroll system, providing they have proper password or other security authorization.
8. Users may not knowingly or willfully create or propagate any virus, worm, Trojan Horse, or other destructive program code.

9. Users may not download or distribute pirated software or data from any source nor any inappropriate images.
10. Users may only download software with direct business use and must take all necessary actions to have such software properly licensed and registered as required. Downloaded software must be used only under the terms of its license.
11. The State has the right to inspect any and all files stored in secured areas of State networks, on computing devices owned or leased by the State, or on any other storage medium provided by the State for State business (i.e. floppy disks, tapes, and RW CDs) in order to monitor compliance with this policy.
12. Authorized individuals, as part of their job responsibilities, may investigate and monitor Internet “links” appearing on State owned web sites to insure linkage to inappropriate or unauthorized web sites does not exist. Discovery of any such violation will result in the immediate deletion of the “link” and a report to the ITA staff for further action.
13. An Internet user can be held accountable for any breaches of policy, security, or confidentiality resulting from their use of the Internet. Such violations of this policy may result in disciplinary action.

V. EXEMPTION PROCESS

Refer to [*Policy 1010 – Information Technology Policies, Standards, and Guidelines Framework*](#).

VI. PROCEDURE REFERENCE

There are no procedure references to this policy.

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

VIII. RESPONSIBILITIES

Users should schedule, wherever possible, communications-intensive operations such as large file transfers, video downloads, and the like for off-peak usage times.

REVISION HISTORY

- 09/03/14 – Revised to include the monitoring and filtering sections
- 07/16/14 – Updated Section I. Authority to be consistent with Idaho statute.

- 07/01/13 – Changed “ITRMC” to “ITA”.
- 6/16/09 – Added Exemption Process and Procedure Reference to this policy; changed the layout and deleted Timeline.
- 11/15/06 – Updated Authority section to reference Executive Order 2005-22. Added new item to Section IV: “Users may not attempt to access prohibited content or to circumvent software put in place by the agency to prevent such access.”

Date Established: October 17, 2001