Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P1000 GENERAL POLICIES

Category: P1050 – EMPLOYEE INTERNET USE, MONITORING, AND FILTERING

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-833
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 responsible Internet usage, and to help employees make best use of State resources. While a direct connection to the Internet is necessary to conduct State business, it can also expose the State to significant risks if appropriate security measures, and responsible use are not employed. Excessive, non-business related Internet usage causes unnecessary network congestion and reduces statewide 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 global network of connected sites and devices accessible through a "web browser" or other means, and provides a wide range of online services and content.

2. Malware - Software that is intended to damage or disable computers and computer systems.

3. Virus – A program or piece of code that is loaded onto a computer without the user's knowledge and runs without user intervention or control. It may contain a self-replicating component to spread the "infection" and will almost always corrupt or modify files on a targeted computer.

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. Information Technology Services (ITS) will monitor and log all Internet activity passing through the State firewall system. Agencies are not authorized to bypass the State firewall system.

B. Internet Filtering

Information Technology Services (ITS) 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. Agencies are not authorized to bypass any State network security system. An agency may elect to employ additional levels of network security based on approval from ITS.

C. Internet Use

1. Access to the Internet is necessary for meeting the business needs of the agency. Internet access is considered to be a State business activity and the agency has the right to monitor the use of such activity at any time. Therefore, users should not have any expectation of privacy related to their Internet usage when conducting State business or when using State resources.

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 pertaining to 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 website for the purpose of conducting State authorized business, such as the online payroll system, providing they have been granted security authorization.

8. Users may not knowingly or willfully create or propagate any virus, malware, or other destructive program code.

9. Users may not download or distribute pirated software, data, or inappropriate images from any source.

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 in order to monitor compliance with this policy.

12. As part of their job responsibilities, authorized individuals may investigate and monitor Internet "links" appearing on State owned websites to insure linkage to inappropriate or unauthorized websites 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 ITA Policy P1010 (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) 605-4064.

REVISION HISTORY

05/30/19 – Modernized terminology and definitions.

07/01/18 – Updated Idaho statute references.

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