Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P1000 GENERAL POLICIES

Category: P1050 – INTERNET USE AND CONTROL

CONTENTS:

I. Authority
II. Abstract
III. Definitions
IV. Policy
V. Exemption Process
VI. Procedure Reference
VII. Contact Information
VIII. Revision History

I. AUTHORITY

Authority: Idaho Code § 67-833
Executive Order 2005-22

II. ABSTRACT

The purpose of this policy is to ensure appropriate and responsible use of the Internet.

III. DEFINITIONS

See ITA Guidelines G105 – ITA Glossary of Terms for definitions.

IV. POLICY

1. Each agency shall ensure all internet activity on agency-owned devices is monitored.
2. Information Technology Services (ITS) shall monitor and log all Internet activity passing through the State firewall system.
3. Agencies shall not bypass any State network security system.
4. ITS shall block access to inappropriate websites and content.
5. An agency may employ additional levels of network security with approval from ITS.
6. Users should not have any expectation of privacy related to their Internet usage when using State resources.
7. Users 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.

8. 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.

9. Users may not attempt to access prohibited content or circumvent controls that are in place to prevent such access.

10. If a user accidentally connects to a site that contains sexually explicit or otherwise offensive material, they must disconnect from that site immediately and report the incident to their supervisor.

11. Use of the Internet as described below is **prohibited** unless explicitly required as part of an individual's officially assigned job duties:

    a. Viewing or distributing obscene, pornographic, or profane material;
    b. Violating laws, rules, or 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. Distributing advertisements for commercial enterprises;
    g. Violating or infringing upon the rights of others;
    h. Conducting business unauthorized by the department;
    i. Obtaining or distributing incendiary statements that 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;
    m. Engaging in activities prohibited by the agency's policies; and
    n. Accessing sites that are known to distribute malware software that is intended to damage, disrupt, or gain access to state resources.

12. Users may not knowingly or willfully create or propagate any virus, malware, or other destructive program code. Users may not download or distribute pirated software, data, or inappropriate images from any source.

13. Users may only download software for 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.

14. 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.

15. As part of their job responsibilities, authorized individuals may investigate and monitor Internet links appearing on State-owned websites to ensure 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 ITS staff for further 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

08/05/24 – Edited policy name from “Employee Internet Use Filtering” to “Internet Use and Control”; moved Definitions to G105 ITA Glossary; revised section 11.

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