State of Louisiana

DIVISION OF ADMINISTRATION
OFFICE OF THE COMMISSIONER

J. "MIKE" FOSTER, JR.
GOVERNOR

MARK C. DRENNEN
COMMISSIONER OF ADMINISTRATION

DIVISION OF ADMINISTRATION

POLICY NO. 3

EFFECTIVE DATE: **January 31, 1994; Revised March 20, 1996; Revised November 15, 1999; Revised May 20, 2003**

SUBJECT: **ACCEPTABLE USE OF INFORMATION TECHNOLOGY SYSTEMS AND NETWORKS**

AUTHORIZATION: **Whitman J. Kling, Jr., Deputy Undersecretary**

I. **POLICY:** Information technology (IT) systems and access to networks, including the Internet/Intranet, are provided only for business purposes of the Division of Administration (DOA). Information Technology Systems and Networks includes, but is not limited to, hardware, software, communications networks, physical facilities, mainframe computer, personal computers and printers, and personal hand held devices.

II. **PURPOSE:** To define acceptable use of information technology systems and networks.

III. **APPLICABILITY:** Applies to all employees within the DOA.

IV. **PROCEDURE:** Employee access and use of information technology systems and networks must be professional and strictly job-related and must conform to the procedures outlined in DOA Policy No. 6 – Use of State Resources. Unprofessional conduct or use of the IT systems and networks for personal pursuits may result in disciplinary action.

V. **ACCEPTABLE/UNACCEPTABLE USE:**

1. Information technology systems and networks are to be used only for legitimate business purposes. Sending or receiving items, such as greeting cards, holiday screen blankers, and entertaining videos are *not* considered job-related activities.
2. All content published is owned by the State of Louisiana and is thus subject to review for cause at any time by supervisory personnel.
3. The content may not express opinions on or violate any workplace discrimination/harassment policy.

POST OFFICE BOX 94095 • CLAIBORNE BUILDING • BATON ROUGE, LA 70804-9095
(225) 342-7000 • Fax (225) 342-1057
AN EQUAL OPPORTUNITY EMPLOYER

4. Materials that are copyrighted, patented or otherwise identified as intellectual property are not to be used without the written permission of the owning or holding sources.
5. Unacceptable uses, which include but are not to be limited to the following, will not be tolerated:
   a. Accessing adult chat sites and adult sites that offer access to sexual/pornographic materials, hate information or racially offensive material.
   b. Engaging in illegal activities or usage for illegal purposes including deliberately sending and/or receiving messages or publishing information that violates State, Federal or local laws and regulations.
   c. Intentionally spreading computer viruses and attempting to or actually gaining unauthorized access to any computers, networks, databases or other electronic information.
   d. Providing personal files or information not related to State business.
   e. Using language considered abusive or objectionable.
   f. Misrepresenting information.
   g. Conducting any activities for profit.
   h. Distributing unsolicited commercial materials.
   i. Soliciting money for prohibited causes such as religious or political issues or campaigns.
   j. Unauthorized deletion and/or modification of data, disruption of IT systems and unauthorized viewing and use of sensitive personal identification data such as social security number, date of birth, phone number, and home address.

VI. RESPONSIBILITY:

The employee is responsible for the appropriate use of information technology systems and networks, and for maintaining the confidentiality of sensitive data to which he/she may have access for the performance of assigned duties.

The supervisor is responsible for determining the level of access an employee needs to perform assigned duties, and monitoring the employee's use of information technology systems to assure professional and job-related use. Possible misuse or violation of policy should be reported to the section head.

Sections are responsible for obtaining and funding any additional internet subscriptions required for access to other computers and networks.

Section Heads are responsible for enforcement of this policy and initiating disciplinary actions as deemed appropriate for violations.