

STATE OF ALABAMA

Information Technology Standard

Standard 630-01S1: Acceptable Use – Prohibited Activities

1. INTRODUCTION:

Inappropriate use of State information technology resources exposes the State and its data to risks including virus attacks, compromise of network systems and services, and legal issues. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these rules and to conduct their activities accordingly. These rules are in place to protect the employee, the State, and the data.

2. OBJECTIVE:

Define inappropriate and prohibited uses of State-owned information technology resources.

3. SCOPE:

These requirements apply to all users (State employees, contractors, vendors, and business partners) of any State of Alabama information system resources.

4. REQUIREMENTS:

4.1 PROHIBITED ACTIVITIES

- Any activity that is illegal under local, state, federal or international law
- Non-incident personal use of State-managed computing resources
- Activities in support of personal or private business enterprises
- Unauthorized reproduction of copyrighted material
- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of software products that are not appropriately licensed for use by the State
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws
- Introducing malicious software (malware) into the network or systems (e.g., viruses, worms, Trojan horses, logic bombs, etc.) within reason of user's control
- Making fraudulent offers of products or services
- Making statements of warranty, expressed or implied, unless part of normal duties
- Accessing, possessing, or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction

- Accessing, possessing, or transmitting any sexually explicit, offensive, or inappropriate images and/or text
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless within the scope of regular duties. Potential disruptions include, but are not limited to, ping sweeps, IP spoofing, and forging routing information for malicious purposes.
- Port scanning, packet sniffing, or other security scanning without prior IT Manager approval
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
- Circumventing user authentication or security of any host, network, or account
- Interfering with or denying service to any user except in the course of assigned duties
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network
- Accessing web sites offering online gambling, games, and related information such as cheats, codes, demos, online contests, role-playing games, traditional board games, game reviews, and sites that promote game manufacturers

4.2 EXCEPTIONS

Employees may be exempted from some of these restrictions in the course of their legitimate job responsibilities (e.g., Investigative personnel may require access to web sites that are otherwise restricted).

IT Managers or Agency Heads shall request exceptions from the appropriate authority (e.g., Network Support, State IT Security Council, or CIO).

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 630-01: Acceptable Use

6.2 RELATED DOCUMENTS

Information Technology Standard 630-03S1: E-Mail Usage

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	12/06/2006	Replaced Standard 630-01S