STATE OF ALABAMA

Information Technology Policy

Policy 630-03_RevA: Email Usage

OBJECTIVE:
Define acceptable and non-acceptable use of the State of Alabama email systems.

SCOPE:
This policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed electronic mail systems.

RESPONSIBILITIES:
State email systems are to be used for business purposes in serving the interests of the government and of the people it serves in the course of normal operations.

Email shall be distributed, stored, and disposed of based on the data content in accordance with State information protection standards.

Personal Use:

Occasional and incidental personal use of State email is anticipated, however, employees and managers are responsible for exercising good judgment regarding the reasonableness of personal use. Personal email shall be deleted or saved separately from work email.

Prohibited Use:

State email systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive (vulgar or pornographic) content or offensive comments about a person's race, gender, age, appearance, disabilities, sexual orientation, political beliefs, or religious beliefs and practices. Employees who receive any emails with this content from any State employee should report the matter to their supervisor immediately. Additional prohibited uses of email shall be addressed in State standards.

Privacy:

Email content created, stored, transmitted, or received using State resources are the property of the State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of email content. Authorized State personnel may access, monitor, or disclose email content for any business purpose or to satisfy legal obligations.

Non-State Email:

Only state-sanctioned email systems are approved for email communications. Direct desktop access to external email systems is not allowed due to the risk of email-borne virus and disclosure of sensitive data. External email systems include personal email boxes as well as access to business partners email systems.

Exception:

Managed clients (systems connected to centrally managed servers providing automatic anti-virus, operating system, and application software updates) may access other web-enabled messaging systems.

ENFORCEMENT:

Refer to Information Technology Policy 600-00: Information Security.

By Authority of:

Chief Information Officer

7/12/06

Date

Policy History

Version	Release Date	Comments
Original	03/02/2006	
Rev A	07/12/2006	Added exception for managed client