

 Georgia Technology Authority	Georgia Technology Authority	
Title:	Privacy in the Workplace	
PSG Number:	SS-12-001.01	Topical Area: Security
Document Type:	Standard	Pages: 3
Issue Date:	April 4, 2012	Effective Date: April 4, 2012
POC for Changes:	GTA Enterprise Governance and Planning	
Synopsis:	No expectation of privacy shall be assumed when accessing non-public State information resources and assets.	

PURPOSE:

The State of Georgia owns or has custodial responsibility for the information accessed, created, transmitted or stored on behalf of the State or in conducting official State business and has ultimate responsibility for protecting that information regardless of the medium used.

The proliferation of non-State technology devices (see definition under Terms and Conditions) entering State facilities and being used to conduct State business has made it essential for the State to develop standards for the appropriate protection of State information.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter, PS-08-005

STANDARD:

A State worker (employee or contractor) shall have no expectation of privacy or information ownership when using a non-State technology device to access, create, process, store, or transmit State information. Such use shall be subject to all federal and State laws and State information security policies and standards including requirements for monitoring and inspection to protect State information assets.

Individuals shall exercise caution when storing personal or other non-State information on non-State technology devices also used to access, create, process, store, or transmit State information.

All agencies shall include education activities in their information security program to ensure all agency workers are aware of this standard as well as all other information security policies and standards that apply to the agency and its staff.

EXCEPTION:

Exempt from the provisions of this standard are:

- The use of non-State technology devices to conduct non-State business or to access the State's public facing web sites or applications.
- State employees accessing State networks from points outside State offices, using non-State technology devices for the sole purpose of conducting personal business such as accessing individual personnel, benefits, medical and/or other private human resources related information (such as but not limited to PeopleSoft Employee Self Service (ESS), Open Enrollment, Leave Tracker, etc.). Accessing these services from within the State premises or State network is not exempt.

Note that State e-mail systems and their contents are property of the State and are not exempt.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Appropriate Use of Information Technology Resources, PS-08-003
- Appropriate Use and Monitoring, SS-08-001
- Media Controls, PS-08-026
- Media Protection and Handling, SS-08-043
- Electronic Communications Accountability, SS-08-009
- Non-State Technology and Computing Devices, SS-12-002

REFERENCES

- NIST Computer Security Resource Center- <http://csrc.nist.gov/> - Special Publications (800 Series)
 - SP 800-53 rev 3 Recommended Security Controls for Federal Information Systems and Organizations
 - PL-4 Rules of Behavior
 - PL-5 Privacy Impact Assessment
 - AC 18 Wireless Access
 - AC-19 Access Control for Mobile Devices
 - MP-3 Media Marking
 - MP-6 Media Sanitization

TERMS and DEFINITIONS

Non-State Technology Devices include but are not limited to: laptops, PDA's, iPods, mp3 players, USB drives, and other portable processing and storage devices not specifically issued or owned by the State of Georgia.

State Information Assets include all data, e-mail and/or information created, accessed, processed, transmitted and/or stored on behalf of official State business that is not otherwise accessible through the public access domains.

State Information Technology Resources (variations: IT Resources or Information Resources) means hardware, software, and communications equipment, including, but not limited to: personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities), and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

Technology devices include but are not limited to laptops, PDAs, mp3 players, ipods, USB drives, and other portable processing and storage devices (regardless of ownership).

Inappropriate usage - see Appropriate Use and Monitoring, SS-08-001.