

 Georgia Technology Authority	<b>Georgia Technology Authority</b>	
<b>Title:</b>	Non-State Technology and Computing Devices	
<b>PSG Number:</b>	SS-12-002.01	<b>Topical Area:</b> Security
<b>Document Type:</b>	Standard	<b>Pages:</b> 4
<b>Issue Date:</b>	April 4, 2012	<b>Effective Date:</b> April 4, 2012
<b>POC for Changes:</b>	GTA Enterprise Governance and Planning	
<b>Synopsis:</b>	Rules of appropriate use and all other governance regarding information and data security apply to non-State issued technology devices used to access <b>non-public</b> State information and technology resources.	

## **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 being used to conduct business on behalf of the State has made it essential that the State establish standards that contemplate their existence and use.

This standard expands upon the rules governing information security to specifically include use of non-State technology devices. It intends to communicate the State's intent and commitment to safeguard sensitive information for which it has responsibility and to discourage the rampant and careless use of non-State technology devices.

## **SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS**

See Enterprise Information Security Charter

## **STANDARD:**

Use of non-State technology devices to perform agency functions is at the discretion of the agency. Agencies shall establish and document internal policies and standards governing the use of non-State technology devices to access non-public State information assets. Such use shall comply with all applicable laws, regulations, policies and standards governing information and data security including but not limited to appropriate use, access, boundary and media controls, records management, retention and e-discovery.

Agencies allowing the use of non-State technology devices shall conduct risk assessments in accordance with State standards, and shall explicitly include the use of non-State technology devices in the appropriate system security plans. When conducting its risk assessment the agency shall consider such items as:

- The State worker already has access to the sensitive information in the course of their duties.
- Possible controls to minimize the impact of lost or stolen devices such as encryption, remote wiping or locking capabilities or GPS tracking.
- Additional compensating controls deployed to minimize new risks.
- Federal requirements that some types of information require the device to be destroyed or wiped to a particular federal standard when the employee no longer has access to the information.
- Laws pertaining to the use of non-State technology devices in the workplace are relatively new and untested in court. The agency should consult with legal counsel regarding their standard and ability to enforce it.

#### **SUPPLEMENTAL EXCEPTION:**

Exempt from the conditions of this standard are:

- All access to the public domain.
- State employees accessing State networks, using non-State 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 ESS, Open Enrollment, Leave Tracker, etc.

#### **RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES**

- Risk Management Framework, SS-08-041
- Appropriate Use of Information Technology Resources, PS-08-003
- Appropriate Use and Monitoring, SS-08-001
- Media Protection and Handling, SS-08-043
- Electronic Communications Accountability, SS-08-009
- Secure Remote Access, SS-08-038
- Tele-working and Remote Access, SS-08-037
- Network Security-Boundary Controls, SS-08-047
- Privacy in the Workplace, SS-12-001

#### **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

## **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.

**Non-Public State Information Assets** include all data, e-mail, and other information created, accessed, processed, transmitted and/or stored on behalf of or in the conduction of official State business, that is not otherwise publicly accessible either through public facing websites or open records.

**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, web sites, 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.

**Inappropriate Usage** - see Enterprise Appropriate Use Standard, SS-08-001.