GTA Georgia Technology Authority	**Georgia Technology Authority**	
Title:	**Password Security**	
PSG Number:	SS-08-007.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 3
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes standards for protecting passwords	

PURPOSE

To establish a standard for protecting passwords and the frequency of change for such passwords to mitigate compromise of sensitive information.

SCOPE

Security standards apply to all agencies, including those executive branch agencies headed by constitutional officers. This standard also applies to all users (employees, contractors, vendors, and other parties) of State information technology systems or data are expected to understand and abide by the Standard.

STANDARD:

All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including but not limited to Administrative Assistants.

Passwords shall not be stored in clear text. Cryptography shall be used to create the stored information.

Users shall not write passwords down or store them anywhere in their office. Nor shall they store passwords in a file on ANY computer system (including Personal Digital Assistants or similar devices) without encryption.

All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) shall be changed every 30 days and all user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed every 45 days. (or not to exceed 6 months if other documented and approved mitigating factors are in effect such as account lockout after a number of logon attempts)

User accounts that have system- level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.

Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.

If an account or password is suspected of being compromised, the incident must be reported to the appropriate access administrator or in accordance with incident response procedures.

Temporary or "first use" passwords (e.g., new accts or guests) must be changed upon first logon the authorized user accesses the system and have a limited life of inactivity before being disabled.

ENFORCEMENT

The State of Georgia enterprise information security policies and standards are based upon the Federal Information Security Management Act (FISMA) and ISO 17799 standard framework of best practices. Individual state agencies are responsible for developing internal procedures to facilitate compliance with these enterprise security policies and standards. The standards are designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence.

Agencies may establish more stringent policies, standards and procedures consistent with this Enterprise standard.

Violations of this standard could result in serious security incidents involving sensitive state, federal, or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

The standards will guide periodic security reviews, as well as audits by the State Department of Audits (DOAA).

AUTHORITY

Official Code of Georgia Annotated (O.C.G.A.) Section 50-25-4 authorizes the GTA to *"establish technology security standards and services to be used by all agencies"* and, to establish and enforce Standard specifications which shall apply to all technology. The Attorney General has opined that such standards apply to and is binding upon all executive branch agencies *including those executive branch agencies headed by constitutional officers*.

EXCEPTIONS

Exceptions to a standard must be approved by the Executive Director of the Georgia Technology Authority Board of Directors, with review by the State Chief

Information Security Officer. In each case, the agency or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. Denials of requests for exceptions may be appealed to the State Chief Information Officer.

GUIDELINES

Passwords should be easy to remember but difficult to guess.

Users should not use the "Remember Password" feature of applications.

User Should Not Employ Any Automatic Log-In Actions

State of Georgia information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources

Where possible, users should not use the same password for different State of Georgia access needs. (For example, a user should select one password for the Engineering systems and a separate password for IT systems.) Also, a separate password should be selected to be used for operating system accounts, unless a Single-Sign-On system is used to control access to multiple systems.

Users should not use the same password for State of Georgia accounts as for other non-State of Georgia access (e.g., personal ISP account, option trading, benefits, etc.).

Use caution when conducting random password audits via the use of automated tools. Internal policies should exist strictly limiting the use and access of these tools to authorized security administrators.

If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any policies.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Password Authentication (Policy)
Strong Password Use (Standard)

TERMS and DEFINITIONS

Authentication is a process of attempting to verify the digital identity of a system users or processes.

Note: PSG number administratively changed from S-08-007.01 on September 1, 2008.