

	<b>Georgia Technology Authority</b>	
<b>Title:</b>	<b>Password Authentication</b>	
<b>PSG Number:</b>	<b>PS-08-006</b>	
<b>Effective Date:</b>	03/20/2008	<b>Review Date:</b> 12/01/2023
<b>Synopsis:</b>	Establishes use of passwords as primary authentication mechanism	

## PURPOSE

Passwords are an important aspect of computer security. They are often the only means for authenticating users and the front line of protection for user accounts. Failure to use a password or using a poorly chosen password when accessing state of Georgia information assets may result in the compromise of those assets. It is the responsibility of every agency to implement authentication mechanisms such as passwords to access sensitive data and the responsibility of the user to appropriately select and protect their passwords.

## SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*

O.C.G.A 50-25-4(a)(21) - *State Government, Georgia Technology, General Powers*

PM-04-001 – *Information Technology Policies, Standards and Guidelines*

PS-08-005 – *Enterprise Information Security Charter*

## TERMS AND DEFINITIONS

**Authentication** - the process of attempting to verify the digital identity of system users or processes.

## POLICY

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to state information systems and applications unless specifically designated as a public access resource.

All users (employees, contractors, and vendors) with access to state information systems shall take the appropriate steps to select and secure their passwords.

## RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Password Security (SS-08-007)

Strong Password Use (SS-08-008)