

Title:	USG Password Authentication Requirement		
Policy Number:	2008-Julian Date	Topical Area:	Security
Document Type:	Issue Specific Policy	Pages:	2
Issue Date:	31-Dec-08	Effective Date:	31-Dec-08
POC for Changes:	USG Office of Information Security		
Synopsis:	Establishes use of passwords as primary authentication mechanism		

PURPOSE

Passwords are an important aspect of information and information technology security. They are often the only means for authenticating users and the front line of protection for user accounts. Failure to use a strong password or using a poorly chosen password when accessing University System of Georgia's information assets may result in the compromise of those assets. It is the responsibility of every Institution and the University System Office 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, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See USG Information Security Program Policy
[See BOR Policy Manual, Section 700](#)

POLICY

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to University System of Georgia and its Institution's information systems, services and applications unless specifically designated as a public access resource.

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

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

USG Password Security (Standard)
 USG Strong Password Use (Standard)

TERMS and DEFINITIONS

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