MIDDLE GEORGIA STATE UNIVERSITY
OFFICE OF TECHNOLOGY RESOURCES

Effective Date: 04/18/2013

Title: Password Policy

1.0 Overview
Passwords are used to access various Middle Georgia State University computer and network resources. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins.

2.0 Purpose
The purpose of this document is to define password construction and protection requirements for users of Middle Georgia State University computer and network resources.

3.0 Scope
This document covers usage of all computer and network systems owned, operated or maintained by Middle Georgia State University.

4.0 Policy
Password Construction
We enforce "strong passwords" as a defense against improper access and compromise of confidential information. When creating a password make sure it is easy to remember and meets the following requirements:

- Must be at least eight (8) characters long
- Must contain characters from at least three (3) of the following four (4) classes:

Description	Examples
English Upper Case Letters	A, B, C, ... Z
English Lower Case Letters	a, b, c, ... z
Westernized Arabic Numerals	0, 1, 2, ... 9
Non-alphanumeric ("Special characters")	!#$%&'()*+,-./:=;<>?@[]^_`|~

- Must NOT contain your user name or any part of your full name
- Must NOT be reused

If you need help creating a strong password, think of an easy to remember phrase, then randomly substitute special characters or numbers for their alphabetic look-a-likes or sound-a-likes. For example, "$" for "S", "0" for "o", "@" for "a", "2" for "to", "1" for "i", etc.

The following are good examples of phrases converted to strong passwords:
My Dog Has Flees > MyD0gH@sFlees
Hello to You > H3llo2u!
Four Score and Seven > 4Score&7

BannerWeb Personal Identification Numbers (PIN)
The BannerWeb application uses PIN numbers which consist of six numeric characters and can not meet the password complexities listed above. Users should however follow the password protection guidelines listed below. Banner GUI will meet this standard.

Password Protection
Passwords must be changed at least every 365 days.

Users should not use the same password for Middle Georgia State University accounts as for other non-Middle Georgia State University access (e.g., personal ISP account, and Instant Messenger account). Where possible, users should not use the same password for different Middle Georgia State University access needs. The exception to this is where a Single Sign On System may control multiple systems.

All passwords should be memorized and treated as sensitive, confidential information. Users should not share Middle Georgia State University passwords with anyone, including administrative assistants or support personnel. 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. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on any computer system (including Personal Digital Assistants or similar devices) without encryption. Passwords should not be inserted into email messages or other forms of electronic communication.

If an account or password is suspected of being compromised, the incident should be reported to the Office of Network Administration and the user should change the password.

Users should not use the "Remember Password" feature of applications and should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

Temporary, or “first use” passwords should be changed the first time that the authorized user accesses the system.

5.0 Enforcement

The Office of Network Administration and other system administrators may perform periodic audits to ensure that passwords are changed at the appropriate time using this standard. System administrators must ensure that their systems require strong passwords by enforcing as many of these characteristics as possible and only issuing strong passwords.

Unit heads will ensure that all staff and faculty are aware of the importance of these policies.

The Chief Information Officer (CIO) must approve any waiver of these requirements.

6.0 Definitions

System Administrator	The person responsible for managing and maintaining a computer system.
PIN	Personal Identification Number

7.0 Revision History

03/24/2004 - Original draft
05/30/2008 - Second draft
04/18/2013 - Changed institution name to reflect consolidation
08/04/2015 - Changed institution name to reflect University status