Policy Number: **612**

Policy Title: **Password Management**

**POLICY:**

A combination of a personal user login ID for identification and a unique password for authentication will be required of all users before they are allowed access to the Georgia Perimeter College network and systems.

**PROCEDURE:** [This is policy, not procedure.]

Passwords will be used for authentication of all access to the Georgia Perimeter College (GPC) network and systems except where stronger authentication methods (such as biometric authentication or two-factor authentication) are deemed necessary. The effectiveness of passwords to protect access to GPC’s information directly depends on strong construction and handling practices.

**Password Construction**

All users must construct strong passwords for access to all GPC networks and systems, using the following criteria:

- Must be a minimum of 8 characters in length, at least 5 of which should be unique
- Must be composed of a combination of at least three of the following four types of characters. When technically feasible use of all four types of characters is recommended (some systems or applications do not accept special (non-alphanumeric) characters in passwords):
  - At least one upper case alphabetic character (A-Z)
  - At least one lower case alphabetic character (a-z)
  - At least one numeric character (0-9)
  - At least one non-alphanumeric character (~, !, @, #, $, %, ^, &, *, -, =, +, ?, [, ], {, })
- Must not consist of:
  - Dictionary (identifiable) words in any language
  - Personal information, such as birthdays, phone numbers, family names, or pet names
  - Passwords which are the same as the user ID
  - Georgia Perimeter College, GPC or any derivation
  - Common letter or number patterns
  - Variations of old or related passwords

Strong passwords can be difficult to remember. One method for creating a strong password that can be more easily remembered is to select a phrase that is meaningful to you but not known by others, use the first letter of each word in the phrase, and add other special characters, numbers, etc. For example:
2 years that will change your life! -- becomes the password -- 2ytwCyl!
(Please do not use this example as your password.)

As an alternate mechanism of password creation, users may construct a complete phrase or sentence containing at least 14 characters (including numeric, special, etc.).

**Password Management**

The following requirements apply to password management.

**Storage and Visibility:**

- Passwords should be memorized, not written down.
- Passwords must not be stored in a manner which allows unauthorized access.
- Passwords will not be visible on a screen, hardcopy, or other device.
- Passwords will not be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.
- Passwords will not be sent via unencrypted e-mail. Neither GPC faculty/staff nor GPC student e-mail is encrypted.

**Changing Passwords:**

- Users must change their passwords at least every 120 days.
- Users who process or access Restricted data (such as protected health information, student FERPA data, and Social Security Numbers or other personally identifiable information) should change their passwords at least every 90 days.
- Users should never rotate through a list of favorite passwords.
- Applications and systems should require that new passwords cannot be the same as the four previously used passwords.
- **Passwords must be changed immediately if any of the following events occur:**
  - Unauthorized password discovery or usage by another person
  - System compromise (unauthorized access to a system or account)
  - Insecure transmission of a password
  - Accidental disclosure of a password to an unauthorized person.
  - Replacement of an account user with another individual requiring access to the same account
  - Password is provided to IT support staff to resolve a technical issue
  - Password is provided to the end-user by the system administrator when establishing a new account or resetting the password

**Password Protection:**

- Passwords must never be transferred or shared with others unless authorized.
- Passwords must not be transferred electronically over the internet using insecure methods.
• When it is necessary to disseminate passwords in writing, the recipient will protect the written password from unauthorized access. After memorizing the password, any written records must be destroyed.
• When transmitting a password orally, measures should be taken to ensure that the conversation is not overheard.
• Use of the “Remember Password” feature on many applications should be kept to a minimum and is highly discouraged.

Password Protection - System Administrators:

OIT system administrators may need to create or disseminate passwords to others. Whenever possible, use a method of password creation that provides the password only to the intended end-user.

OIT system administrators must implement the following to deter password cracking:

• An automated method to mitigate “brute force” password attacks should be used. For example, some systems will lock an account for a few minutes after several failed login attempts.
• Logging must be set up to record all failed login attempts and selected successful attempts as well.

Password Protection – Application Developers:

• Application developers must use secure authentication methods, whenever possible.
• Creating applications which store passwords should be avoided. If password storage cannot be avoided, developers must ensure that applications do not store passwords in clear text or in a readily decrypted form.
• Applications should support unique logins. Password sharing should not be allowed.

Compliance and Enforcement

The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users. Persons in violation of this policy are subject to a range of sanctions (determined and enforced by GPC management), including the loss of computer network access privileges, disciplinary action, dismissal from the college, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws. The college will carry out its responsibility to report such violations to the appropriate authorities.

PPAB Approval Date: ________________________________

Policy Council Review Date(s):

ITPC: 08/24/12