Title of the Policy: Password Policy

Functional Area: IT Services

Applies To: All users and service providers of Armstrong’s Information Technology resources and services.

Policy Reference(s):
- USG IT Handbook Section 5.12
- Responsible access and use of Information Technology Resources and Services policy

Number:

Date First Issued: April 2017

Date Last Reviewed:

Page(s): 2

Responsible Person
CIO, Information Security Officer

Purpose / Rationale

The purpose of this policy is to establish standards for creating, protecting, and changing passwords. This policy is guided by an overarching Password Policy mandated by the University System of Georgia, noted in USG IT Handbook Section 5.12.

IT Security and regulatory compliance require that we enforce password policies throughout our infrastructure, ensuring password policies are implemented on enterprise apps as well as cloud apps and on managed devices.

This policy should be taken into consideration for all technologies implemented hereafter. IT Services will work with vendors to enforce an appropriately complex password within the technical environments and limits.

All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators, vendors, and all other parties.

Definitions

Password – a secret word or phrase that must be used to gain admission to something.

Passphrase - a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

Clear text - the form of a message or data that is immediately understandable to a human being without additional processing.
Policy

Password Requirements:

All user level passwords shall be changed every one hundred and eighty (180) days. User level passwords are used to access resources such as Campus Computers, Port of Armstrong, Email, etc.

Additionally, users with administrative privileges to specific systems sponsored by IT Services must change their passwords to those systems every ninety (90) days. (An example of these systems include but are not limited to: PCI based systems, Blackboard, StarRez).

a. Passwords must exhibit complexity by having the following characteristics:
   i. Be at least ten characters in length
   ii. Must not contain user’s name or part of the user’s name
   iii. Must not contain easily accessible or guessable personal information about the user or user’s family (e.g. birthdays, children’s names, addresses).
   iv. Must contain at least three of the following character types:
      (a) English uppercase (A-Z)
      (b) English lowercase (a-z)
      (c) Numbers (0-9)
      (d) Non-alphanumeric special characters ($, !, %, ^, …)

2. Password history must be enabled to disallow usage of the same password for a length of 4 change cycles.
   a. This means that users will not be allowed to use the same password that has been used in the past 5 changes.

3. Passwords shall not be stored in clear text.

4. Users shall not write passwords down or store passwords anywhere in their office or publically. They shall not store passwords or passphrases to systems and resources noted in a file on any computer system, including smart devices, without encryption. Password management utilities can be used to securely track your passwords as they are kept in an encrypted vault and not in clear text.

5. 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.

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

7. If an account or password is suspected of being compromised, the incident must be reported to the IT Services.

8. Temporary or “first use” passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system, and have a limited life of inactivity before being disabled.

9. Users who have changed their user password must not be allowed to change password immediately following. This will deny users the ability to get back to their old password.