The American College of Greece
Password Policy

Introduction and purpose

Passwords are one of the most important aspects of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of ACG's resources. All users, that have access to systems and services of ACG, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes everyone who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides (physically or logically) at any ACG facility, has access to the ACG network, or stores any non-public ACG information.

Technological resources are provided by the College to support its primary role of education, research and associated functions related to this role.

The College complies with, and adheres to, all its current legal responsibilities including under Data Protection, Electronic Communication and Intellectual Property legislation.

Responsible College Office & Officer

The Office of Information Resources Management (IRM) is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Executive Director for IRM is the responsible officer.

Who is governed by this policy?

This policy applies to all individuals who are granted access to ACG Technological Resources. Those individuals covered include, but are not limited to, faculty, staff, students, alumni, those who are working on behalf of the College, and/or individuals authorized by affiliated institutions and organizations.

Exercising access to any ACG technological resource automatically signifies acceptance of this policy.

Procedures

Passwords can be changed ONLY by the respective user. Passwords CANNOT be changed over the phone or supplied through e-mail. If a user has lost any means of accessing his/her account, must contact the IT department in person so the password can be reset.

I. Password Creation Policy

- All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
- Users must not use the same password for ACG accounts as for other non-ACG access (for example, personal ISP account, banks, benefits, and so on).
- Where possible, users must not use the same password for various ACG access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

II. Password Change

- All system-level passwords (for example, root enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every three months.
- Previously used passwords must not be re-used unless a significant amount of time has passed (four months) or at least two other passwords have been used.
- Password cracking or guessing may be performed on a periodic or random basis by the IT Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.
- Password creation and changes in respect to this policy **WILL** be system observed and enforced.

III. Password Protection

- Passwords **must not** be shared with anyone. All passwords are to be treated as sensitive, Confidential ACG information.
- Passwords **must not** be inserted into email messages, documents or other forms of electronic communication.

- Passwords **must not** be revealed over the phone to anyone.
- Passwords **must not** be revealed on questionnaires or security forms.
- **Do not** hint at the format of a password (for example, "my family name").
- **Do not** share ACG passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- **Do not** write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- **Do not** use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised **must report** the incident and change all passwords.

IV. Application Development Activities

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

V. Password Construction Guidelines

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters (**Required**).
- Contain both upper and lower case letters (**Required**).
- Contain at least one number (for example, 0-9) (**Required**).
- Contain at least one special character r (for example,!$%^&*()_+|~-=\ `{}[]:";'<>?,/). '<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family

members, pets, friends, and fantasy characters.

- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily but others are difficult to guess. One way to do this is create a password based on a song title, affirmation, or other phrase that has a special meaning to the user. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

VI. Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lower case letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases

VII. Password Expiration

Passwords will expire automatically after a period of 180 days. All users will receive appropriate email notification as the password expiration day approaches.

VIII. College Monitoring

IRM specialists frequently monitor network and computer systems access and utilization. This is done for various purposes which include: assessing systems availability and performance; identifying and resolving technical problems; to detect computer viruses, spyware, file-sharing software, etc. and/or to detect prohibited activities; to enforce College administration’s directives and/or orders properly issued by law enforcement and legal authorities.

In any investigation of misuse, the College may inspect, without prior notice, the contents of files,

voice mail, logs, and any related computer-generated or stored material, such as document output;

Account holder's computer files may be inspected occasionally when assuring system integrity or performing related authorized resource management duties.

IX. Violations

If any user does not adhere to this policy, the College reserves the right to take any and all actions provided by the law, including, without limitation, disciplinary action, termination of employment contracts, where applicable, etc. Questions regarding the application of this policy should be directed to the Office of Information Resources Management.

X. Definitions

Computer Network - Two or more computers that can share information, typically connected by cable, data line, or satellite link.

SNMP - Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

Dictionary attack - attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password. Dictionary attacks are often successful because many users and businesses use ordinary words as passwords.

Technological Resources – Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the College which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, technologies equipped college residencies and computer furnishings operated or maintained by ACG.

Users – Faculty, staff and students as well as others who have been authorized to use The American College of Greece technological resources, i.e. contractors, interns, volunteers, etc.

Contacts

For questions or comments:

The American College of Greece
Information Resources Management Department
Web: http://www.acg.edu/information-resources-management
Email: acgirm@acg.edu
Telephone: +30 210 600 9800 ext. 1356

Policy Changes

The Executive Director for IRM is charged with the responsibility to periodically review the policy and propose changes as needed.

Date of Creation: December 10, 2016
Date of Last Update: March 16, 2018