

Password Protection Policy

- Reference:** CNS-P-I-PASSWORD **Revision:** A
- Supersedes:** None
- Purpose:** The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.
- Source:** Computing and Networking Services (CNS).
- Approved by:** Nabil Bukhalid, Director of CNS **on:** August 28, 2007
Peter Heath, Provost **on:** Pending
- Applicability:** This policy applies to all computer users.
- Background:** Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees, faculty and students of AUB are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.
- Scope:** This policy applies to all employees, faculty and students of AUB who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any AUB facility, has access to AUBnet network, or stores any non-public AUB information.
- All employees, faculty and students are subject to this policy and required to abide by it.
- Policy:**
- 1. Passwords must be changed every 6 months.**
 - 2. Changed passwords cannot be re-used immediately.**
 - 3. Users will be notified 2 weeks in advance of password expiration date. If system permits, users will be prompted to select a new password.**
 - 4. All passwords must conform to the guidelines outlined below.**

Guidelines: Password Construction Guidelines:

Passwords are used to access any number of company systems, including the network, e-mail, the Web, Students Information System and Financial Information System. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords must contain at least 6 characters.
2. All passwords must start with a letter.
3. Wherever possible passwords must contain at least one uppercase letter (e.g. N) and 3 lowercase letters (e.g. t).
4. Passwords must contain at least one numerical character (e.g. 5).
5. Wherever possible passwords must contain at least one special character such as (e.g. \$).
6. A new password must contain at least 4 characters that are different than those found in the old password which it is replacing.
7. Passwords should not be based on well-known or easily accessible personal information. or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.
8. Passwords must not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.
9. Passwords must not be based on publicly known fictional characters from books, films, and so on.
10. Passwords must not be based on the company's name or geographic location.

Password Protection Guidelines:

1. Passwords should be treated as confidential information. No employee, faculty or student is to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members, under any circumstances.

2. If someone demands your password, refer them to this policy or have them contact CNS.
3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to AUBnet resources via AUBnet IPsec-secured Virtual Private Network or SSL-protected Web site.
4. No employee, faculty or student is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.
5. Do not use the “Remember Password” feature of applications.
6. Passwords used to gain access to AUB systems should not be used as passwords to access non-AUB accounts or information.
7. If possible, don’t use the same password to access multiple AUB systems.
8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to CNS and the password changed immediately.
9. AUB may attempt to crack or guess users’ passwords as part of the IT security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Enforcement: Any employee, faculty or student who is found to have violated this policy may be subject to disciplinary action, up to and including termination of AUBnet account privileges or termination of employment.