Password Management

Arkansas School For Mathematics Sciences & The Arts (ASMSA) uses information technology to provide services to the schools users and to run ASMSA educational and business functions. Since username and password combinations are the primary method of protecting ASMSA systems against unauthorized use, ASMSA developed this policy to define general rules and responsibilities.

Scope

This policy applies to all the users, including but not limited to students, faculty, staff, contractors, and services, systems, infrastructure, and components providing ASMSA services to users.

Guidelines

- Every user is expected to change any pre-assigned default password at the first possible opportunity, to select strong passwords that are difficult to guess, and to safeguard them from casual observation or capture.
- Every password for ASMSA-provided accounts should be changed at least twice a year and for greater security, it is recommended to be changed even more often.
- New password should not be the same with the previous 20 passwords.
- Accountholders should not use any of their university passwords as the password for a social media site, or a personal banking site, or other outside resources.
- Users should not use “auto-store” features provided by web browsers or applications.
- Every user must select quality passwords with sufficient minimum length. A quality password must have the following qualifications:
    - Must be easy to remember,
    - Must be at least 12 characters long,
    - Must contain both upper- and lower-case letters, at least one number (for example, 0-9), and at least one special character (for example, $%^&*() _+|~-=\`{}[]:";'<>?,/)
    - Must not be based on anything somebody else could easily guess or obtain using person related information, e.g., names, telephone numbers and dates of birth etc.
    - Must not be vulnerable to dictionary attacks therefore should not be a single word that can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
    - Should not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

  - Should not contain work-related information such as building names, system commands, sites, companies, hardware, or software.
  - Should not contain repeating letters and numbers or letter and number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
  - Should not contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret)
  - Must be free of consecutive identical, all-numeric or all-alphabetic characters.
  - If it is temporary, must be changed at the first log-on.
  - Must not be shared with anybody.
  - Must be properly protected when they are used in automated log-on procedures and are stored.
- 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.
- All system-level passwords (for example, root, enable, system admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
- To protect your password:
  - Do not reveal a password on questionnaires or security forms.
  - Do not hint at the format of a password (for example, "my family name").
  - Do not share ASMSA 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 reveal the password over the phone to anyone, including IT Services.
  - Do not insert password into email messages, alliance cases or other forms of electronic communication.
- Applications can not contain pre-determined static passwords.
- IT Services may perform password cracking or guessing on a periodic or random basis. 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 this policy.
- Users are responsible for any usage of their usernames and passwords. Users must keep their passwords confidential and not disclose them.
- Passwords must not be embedded into applications.
- Every user should take reasonable measures to prevent their accounts, usernames, and passwords from being used by others.
- Every password must comply with password management policy.