I. POLICY STATEMENT

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password may result in the compromise of University systems, data, or the network. As such, all UMass Lowell students and employees (including contractors and vendors with access to university systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Under no circumstances should a user divulge their password to another person. Doing so is a violation of the University’s Acceptable Use Policy and Information Security Policy.

II. PURPOSE

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.

III. SCOPE

The scope of this policy includes all users who have or are responsible for an account (or any form of access that requires a password) on any computer that resides at any UMass Lowell facility, that has access to the UMass Lowell network, or stores any non-public UMass Lowell information.

A. Minimum Password Requirements (all University accounts)
   a. Passwords must have a length between eight (8) and sixteen (16) characters
   b. Passwords must include only 3 out of 4 of the following:
      c. Contain at least 1 upper-case character
      d. Contain at least 1 lower-case character
      e. Contain at least 1 special character (i.e., @!#$%^&*)
      f. Contain at least 1 numeric character
   g. The only valid special characters are: ` ~ ! @ # $ % ^ & * ( ) _ + = { } | \ [ ] \
   h. Passwords cannot include a space
   i. Passwords cannot contain all or part of your email address
   j. Passwords will be locked out for 15 minutes after 5 consecutive invalid login attempts
   k. Passwords will expire after 180 days
   l. You must wait 10 days before changing your next password
m. Passwords cannot be re-used

B. Elevated Privileged System Accounts

Elevated privilege system accounts (are those accounts that have the rights required to maintain a system or application – such as operating system, application, or database administrator accounts, or to operate a scientific instrument. Administrators should not use their standard UMass Lowell AD user account as an elevated privilege system account. Each systems administrator should be assigned their own elevated privilege system account that is not shared, and is used only when the elevated privileges are required. Where possible, these accounts should use a managed authentication service such as Active Directory, LDAP or RADIUS. When elevated privilege system accounts are accessed remotely, it is required that they are used as part of a multi-factor authentication service.

Elevated privilege system account passwords/passphrases will:

- comply with the minimum password standards
- be changed at least semi-annually every 180 days
- be at least 16 characters in length when possible

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. All system-level passwords (e.g., root, enable, Windows Server admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.

C. Local workstation administrator accounts

Special requirements above also apply to local system administrator accounts where the password is stored on the workstation or network device and account authentication does not rely on a central authentication service. Local administrator passwords should be unique per computer or network device and must not be the same as the user’s LDAP account. The local administrator account and password should only be used for system administration purposes.

D. Service accounts

These are accounts where the password is managed within a work group, and include device passwords. Service accounts are subject to the elevated privilege account password complexity requirements but are exempt from the change requirement. These accounts should be reviewed annually to ensure that they are still required for proper operation. All service account passwords must be changed when a work group member who could have known the service account password leaves the work group.

E. Additional Requirements

a. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.

b. All temporary passwords must be changed at first logon.

c. Where 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. A keyed hash must be used where
available (e.g., SNMPv2).

d. Assisted Password Resets
User account passwords will not be reset if the password administrator cannot identify the user requesting the password change/reset with one of the following:
  o A secret key or satisfactory answers about personal information held in central database records
  o A supervisor or technology support person’s personal vouch/identification
  o A photo ID or human factor such as a biometric scan, or
  o Satisfactory challenge-responses in a self-service university-approved password management application

F. Enforcement

All computer systems and processes subject to this policy are encouraged to incorporate a managed University authentication service for automated account and password management, or they must implement the password standards locally. Systems and processes that do not comply with this policy, and have not been granted an exception, will be subject to loss of access to the University campus network.

IV. DEFINITIONS

Computer – Any server, desktop, or laptop running Windows OS, Linux/Unix OS, or Mac OS

V. PROCEDURES

Policy Exception Process

University applications or services with an implementation that do not meet the minimum password standards must be granted a policy exception. The approval process for exceptions requires the system owner to share a technical description and statement of justification for the exception. This information, and if necessary a security review, are subsequently analyzed and approved by the University’s Information Security Officer. E-mail: infosec@uml.edu for more information.

This policy will be reviewed and updated every three years, or earlier as needed for compliance reasons, in accordance with the University Policy for Creating and Establishing UMass Lowell Policies

VI. RESPONSIBILITY

Information Technology is the responsible organization for implementing the provisions of this policy. The University’s Chief Information Officer and the Information Security Officer are the designated point of contacts.

VII. ATTACHMENTS

None
VIII. RELATED POLICIES, PROCEDURES AND ANNOUNCEMENTS

Acceptable Use Policy, IT-5-101

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.