



Information Technology Standards

UNM Account Password Standard

IT Standard Issued: 06/05/2007

Supersedes: This is a new Standard.

Responsible Executive: CIO.

Responsible Office: Office of the CIO.

Contact: For questions about this standard, please contact The Office of the UNM Information Security Administrator. To report violations of this standard, please call the IT Security Incident hotline at 1-505-277-0930.

Summary of Standard: UNM is committed to protecting the privacy and security interests of the UNM community. This standard defines expected practices for creating and changing passwords in the interest of meeting this obligation. All members of the UNM community must follow these standards to be in compliance with UNM policy.

Who is Affected by this Standard: Every individual associated with UNM who creates, uses, or changes a password that is used to access UNM information assets. Individual account users must follow this standard, even if it is not technically enforceable; System Administrators must apply technical controls to enforce this standard, where possible.

Why We Have this Standard: This standard improves the University's security posture for computer systems through the codification and adoption of industry best practices. Poor password habits may impact the confidentiality, integrity and availability of University business systems and of other sensitive electronic information.

Responsibilities: Every individual associated with UNM is responsible for selecting a strong password for his or her account, and for regularly changing that password. The CIO's Office is responsible for modifying these standards.

Procedures:

- All passwords **must** contain upper and lower case characters and numbers or symbols. When setting a password on a system not capable of this minimum standard, individual users **must** use as complex a password as possible for that system.
- All passwords **must** be changed any time a compromised machine or site has been used where a password has been entered.

- All account holders **must** agree to abide by this standard, and by all other UNM policies, before being granted access to UNM systems, unless the account holder is covered by another agreement, such as a business associates agreement.
- Passwords **must not** include dates that are personally relevant, such as dates of birth, office or phone numbers, or social security numbers.
- Passwords for individual accounts **must not** be shared.
- Common-use or departmental accounts may have credentials shared provided the account **must not** be used to access UNM business information outside of the department or UNM business unit.
- All individuals **should** select good passwords for the systems to which they have access.
- All individuals requiring access to sensitive information **should** complete information security training covering the handling of that sensitive information before being granted access to such information.
- All passwords **should** be changed every 180 days or sooner. All passwords to accounts that provide access to sensitive information **should** be changed every 90 days or sooner. All accounts with expired passwords **should** be locked.
- Accounts **may** be locked out after five failed login attempts within 5 minutes.

Website Address for this Standard: <http://cio.unm.edu/standards/>

Related Documents: UNM Policy 2510 Section 4.1 “Computer Use Guidelines” (<http://www.unm.edu/~ubppm/ubppmanual/2510.htm>), Policy 2520 Section 2.1.1 “Computer Security Controls and Guidelines” (<http://www.unm.edu/~ubppm/ubppmanual/2520.htm>).

Keyword Index: user account, shared account, password, information security, information assurance, authentication.

Appendices: None.