NMSU Password Standard for General Users

Purpose of this Standard

This document sets forth password requirements for all NMSU individual user accounts. All passwords used to access computing devices that connect to the University network must meet the specific minimum password requirements described below and must be traceable to individual users. Any suspected compromise of a password must be reported immediately to NMSU's CISO. This standard does not supersede any unit or departmental password standard that imposes more stringent requirements for general users than the minimum requirements set forth herein.

Audience

Any faculty member, staff member, student, temporary employee, contractor, outside vendor, or visitor to campus ("User") who has access to NMSU owned or managed information.

Standard

A user's password must:

- Be 8 to 16 characters in length
- **NOT** contain the username (or more than three consecutive characters of the username)
- **NOT** contain spaces or non-English characters
- Contain **AT LEAST one** UPPERCASE letter: A - Z
- Contain **AT LEAST one** lowercase letter: a - z
- Contain **AT LEAST one** number: 0 - 9
- **Do NOT** use 3 or more repeated (i.e., aaa or 111) or consecutive (i.e., abc or 123) characters
- **ONLY** the following special characters are allowed: _ { } | [ ]

Password Sharing:
All passwords are to be treated as confidential sensitive information. Passwords will not be shared with others. Examples of unauthorized sharing include sharing passwords with supervisors, administrative assistants, coworkers or spouses.

General Password Rules:

- Users will only use account credentials for which they have been authorized.
- Use of standard user accounts to run system services is prohibited.
- Users may not attempt to "crack" (decrypt) encrypted or hashed passwords without the explicit written permission of the Information Security Office.
- A password will never be inserted into plain text emails, stored unencrypted in computer files, or written down.
- Password reuse is prohibited.
- A password will not include personal information, such as Social Security number, name or date of birth.

- All users are responsible for maintaining the security of their passwords. In the event that an account is believed to have been compromised, the person detecting the incident should report the incident immediately to the CISO at ciso@nmsu.edu or Helpdesk. In addition, the responsible system administrator should be contacted directly and informed about the password compromise. An account is deemed compromised if it is known or reasonably suspected that the account is being used by an unauthorized party. A compromise will affect the functionality of any account, and the account will not be restored until the risk associated with any such compromise has been mitigated.
- Vendor-supplied default and/or blank passwords shall be immediately identified, reset and changed upon installation of the affected application, device, or operating system.
- Passwords expire within 120 days and each user is required to reset them before expiration.

Lock-Out:
After 30 failed attempts to log-in, the system will lock-out a user for 30 minutes. After 30 minutes, users may attempt to log in again. Each system will be locked out automatically after 30 minutes of inactivity.

Compliance

Failure to comply with this standard may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with NMSU.

Violation of this standard may also carry the risk of civil or criminal penalties.

Roles and Responsibilities

Users shall comply with NMSU's password standards listed in this document. Departments may employ more stringent password standards than those outlined in this document, but not less stringent than those listed here. NMSU's CISO may accept the risks related to technical system limitations through the completion of a Risk Acceptance Form (RAF).

Definitions:

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges.
Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Password: A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.
Password Circulation: An attempt to bypass the basic password requirement that prohibits reusing the same password within a specified period of time by changing the password

repeatedly within a brief period of time in order to be able to reuse the password earlier than intended.
Unauthorized Access: Occurs when a user, legitimate or unauthorized, accesses resources that the user is not permitted to use.
Sensitive Information: is defined as information that is protected against unwarranted disclosure.

Guideline ICT Helpdesk – resetting password standard

Caller calls helpdesk because they have forgotten their password.

The helpdesk asks if they know their Aggie/Banner ID. If they don't, then other questions are asked as per below to verify their identity (address, cell#). The helpdesk does not give them their banner#.

If caller doesn't know their user name/e-mail, they are sent to the my.nmsu.edu login portal, and right below where they login there is a "forgot your user name" link where callers can retrieve their information using their SSN -or- NMSU ID Number and Date of Birth.

Questions to verify identity
1. Ask the customer if they are, in fact, the account holder (you can notify them that impersonating another person's identity is a felony offense).
2. Ask the customer their Aggie/Banner ID.
3. Ask the customer their date of birth.
4. Ask the customer the last four digits of their Social Security Number.

Passwords reset by the Helpdesk*
5. During business hours (M-F, 8 am - 5 pm), reset the password to 'Aggiesxxxxxx' where xxxxxx = the last six digits of their Aggie/Banner ID.

OR

5. During after hours (M-S, 5 pm - 8 pm), if they do not know their Aggie/Banner ID, xxxxxx = the day's date (mmddyy).

***** - Callers are sent a temp password via e-mail and the helpdesk strongly recommend callers to change their temporary passwords immediately.