NMSU Password Standard for Privileged Accounts
System, Network and Application Administrators or User Accounts with Elevated Access

Purpose of this Standard

This document sets forth password requirements for all system, network and application administrators or User Accounts with Elevated Access. All passwords used to access computing devices that connect to the University network must meet the specific minimum password requirements described below. 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 system, network and application administrators than the minimum requirements set forth herein.

Audience

All employees formally fulfilling the duties of System, Network and Application Administrators or User Accounts with Elevated Access.

Standard

- A user account that has system level ("administrator") privileges or programs such as "root" access shall have a different password from all other accounts known by that user.
- A user account that has system level ("administrator") privileges or programs such as "root" access must have its password expiration period set to at maximum180 days or the user of such an account may use two-factor authentication as an alternative and be able to expand the expiration period to 365 days.
- Minimum Password Length: 16 characters
- If an employee has dual roles as user and administrator, whenever possible, the employee should log into the account with the least privileges to perform their work.
- As an exception to the 180-day password expiration, a password on an administrator account must be changed whenever the administrator responsible for the account leaves the organization or changes roles.
- Follow complexity requirements applicable to normal user accounts
- Systems must be configured to log all log-in attempts (successful and unsuccessful). Where technically feasible, logging should be configured to include NMSU system name, system account name, remote computer information such as IP address or remote computer name, and relevant time and date information. Logs must be retained for a minimum of 90 days.

Standards for Service Accounts, Specialty Devices, and Password Management Software or Spreadsheets

Service Accounts: Service accounts are system/device accounts used to run IT services for applications (e.g., web services, database services) and not used regularly by administrators. The password length and complexity requirements are increased to allow for

less frequent password expiration that may be appropriate to ensure that key services are not disrupted due to password expiration.

- Service accounts specifically created for services/applications must only be used for system services. Use of a standard user account to run system services is prohibited. End users and administrators are not allowed to remotely log in using service account credentials except as needed in the scope of supporting the specific service. Systems/devices should be configured to prevent remote logins to service accounts wherever technically feasible.

The following password standards apply to service accounts:

- Password Expiration: 365 days
- Minimum Password Length: 16 characters
- As an exception to the 365-day password expiration, a password on a service account must be changed whenever the staff responsible for the account leaves the organization or changes roles.
- Lock-out Period: N/A
- A password must contain at least one upper or lower case letter and at least one numerical digit, and a special character.

Examples of service accounts:

- Web service account created and used to run a web service
- A database account created to run a database service
- An application account created to run a specific application

Specialty Devices: Due to the wide variety of specialty devices and their frequently limited capabilities, particularly with regard to password management, specialty devices such as fax machines, printers, physical access control equipment, copy machines, specialty lab equipment, phones, projectors, etc., are not subject to this standard other than being required to change their default password to a password that meets this standard or *unless* those devices are used to store or protect sensitive information or perform mission-critical functions. Where appropriate, departments should develop their own specific standard for the specialized devices they use to ensure that adequate authentication controls are present but should not be less stringent than this standard. Technical limitations to meeting this standard should be clearly documented and approval from the institution's CISO is required for any deviations through the completion of a Risk Acceptance Form (RAF).

Password Management Software or Spreadsheets: Passwords may not be written down or stored in clear text, although password management software may be used as long as it employs a minimum of AES128 encryption or stronger. Spreadsheets being used to track passwords must have the latest patches and use password encryption. The passwords used to access this software or spreadsheet application must meet the requirements set forth in this standard.

Compliance

Failure to adhere to these password standards may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of

employment. Contractors and vendors who fail to adhere to this standard may face termination of their business relationships with the University.
Violation of this standard may also carry the risk of civil or criminal penalties.

Roles and Responsibilities

System, Network and Application Administrators: Ensure password standards outlined in this standard are met and maintained and the University's Policy for General Users is followed.

Definitions:

Administrator (System, Network or Application): Generally, a staff member that manages and maintains computer devices for the University and is authorized to have access beyond that of an end user.

Elevated Access: Elevated privileges is when a user is granted the ability to do more than a standard user such as administering IT equipment and/or having access to a vast amount of sensitive data.