WESTERN
NEW MEXICO UNIVERSITY

POLICY NAME	Password & Authentication Policy	**POLICY NO.**	BA469
APPROVING BODY	Cabinet/President	**VERSION NO.**	01
RESPONSIBLE DEPARTMENT	Business Affairs – Information Technology		
EFFECTIVE DATE	Date	**REVIEW/REVISION DATE**	NEW

PURPOSE:

This policy outlines the minimum requirements for passwords, passphrases, multi-factor authentication, and authentication controls used to access university information, systems, applications, networks, and services. These requirements are meant to prevent unauthorized access, reduce credential related security incidents, and protect institutional and personal information.

PASSWORDS AND AUTHENTICATION POLICY:

All employees, students, and affiliates including contractors, vendors, consultants and other authorized third parties shall when accessing institutional information systems, cloud services, applications, networks, or managed devices using standard user, privileged, service, emergency, or other accounts capable of authenticating to institutional systems adhere to the requirements below.

PASSWORD REQUIREMENTS

MINIMUM LENGTH

- A minimum of 15 characters for passwords used as a single authentication factor.
- A minimum of 12 characters for passwords used as part of multi-factor authentication process
    - To the best of its ability the Information Technology Department will support password length up to 64 characters and full password verification without silent truncation

PASSWORD COMPOSITION

- Users are encouraged to use long, unique passphrases or randomly generated passwords.
- Some, but not all university systems may require the inclusion of uppercase letters, lowercase letters, numbers, and symbols.

All policy approvals and revision history are maintained in the Policy Office. Draft and archived/obsolete revisions are not to be used. Please refer to the WNMU website @ https://policy.wnmu.edu for the current approved version of the policy.

PASSWORD REUSE

- Passwords must be unique to individual accounts and services. Users shall not reuse institutional passwords across multiple services, for personal accounts, or reuse personal passwords for institutional accounts.
    - Immediate reuse of passwords will be restricted by technical controls where supported and appropriate.

CHANGES TO PASSWORD REQUIREMENT

- Should the need to increase the minimum requirements of the password standards listed above due to system changes or for the purpose of security, the Information Technology Department may implement such changes at any time to maintain the security of university information, systems, applications, networks, and services. Any changes will be communicated to the campus community via university email and subsequently submitted for formal review at the next available policy review cycle.

PASSWORD CHANGES

- Passwords shall be changed when:
    - There is evidence or a reasonable suspicion that the password has been compromised.
    - The Chief Information Officer or authorized incident-response personnel direct a change as part of incident containment.
    - A temporary or initial password must be replaced during account activation.
    - A change is required by an applicable law, contractual obligation, or documented risk determination.

ACCOUNT PROTECTION AND ACCEPTABLE USE

- All users shall:
    - Keep passwords and authentication factors confidential.
    - Never share personal credentials or approve authentications prompts they did not initiate.
    - Never send passwords through email, messaging, or other unapproved communication channels.
    - Use institutionally approved password managers where available and as deemed appropriate.
    - Avoid storing passwords in plaintext, unprotected documents, scripts, or other insecure locations.
    - Protect recovery codes and authentication devices.
    - Report suspected phishing, unauthorized authentication prompts, lost authentications devices, and suspected credential compromise immediately.

PRIVILEGED, SERVICE, AND NON-HUMAN ACCOUNTS

- Privileged accounts will be maintained separate from standard user accounts wherever possible. Privileged access will be restricted to authorized personnel for legitimate duties.
- Service accounts shall have a documented owner, specific business purpose, defined permissions, and be stored using an approved credential management system.
- Account secrets, API keys, tokens, certificates, and other non-human credentials will be stored in an approved secret management system or equivalent protected mechanism. Default credentials shall be changed or disabled before a system enters production.
- Non-human credentials shall be rotated or replaced following the Password Changes section above or as required by individual systems. Credentials that are exposed or suspected of compromise will be revoked or replaced promptly.
- Emergency accounts will adhere to all standards above and be restricted to approved use only.

MULTI-FACTOR AUTHENTICATION

- Multi-Factor Authentication (MFA) will be required for all users including privileged and administrative accounts.
- MFA will be required for remote access to institutional systems, except where approved architecture provides an equivalent control.

INFORMATION TECHNOLOGY SAFEGAURDS

- The Information Technology Department shall implement appropriate controls, including:
    - Secure transmission of authentication credentials.
    - Ensuring approved credential storage services utilize salted password hashing mechanisms.
    - Monitoring and alerting for suspicious authentication activity.
    - Session and token revocations as needed to contain compromised accounts.
    - Appropriate account provisioning, deprovisioning, and access review.

EXCEPTIONS

- Any requested exceptions shall be documented and subject to compensating controls, and periodic review.
- Requests should include:
    - The system, account, and requirement for which an exception is being requested
    - The business or academic justification
    - The applicable technical limitation or conflicting obligation
    - Proposed compensating controls
    - A listed owner, review date, and/or expiration date
- Requests will be reviewed and approved or disapproved by the Chief Information Officer or their designee

- Exceptions shall not be open-ended, reviewed at least once every twelve months, and revoked when no longer needed.

COMPLIANCE AND ENFORCEMENT

- Violations of this policy may result in access restrictions, account suspension, required remediation, or complete loss of access to the associated systems or services.

DEFINITIONS

- Authentication: Verification of a user's or system's identity before access is granted.
- Password or passphrase: A secret used to authenticate an identity or to activate an authentication mechanism.
- Multi-factor authentication (MFA): Authentication using at least two distinct factor types.
- Privileged account: An account with administrative or elevated permissions capable of changing systems, security controls, accounts, or protected data.
- Service account: A non-human identity used by an application, process, integration, or service.
- Compromised credential: A credential suspected or confirmed to have been disclosed, stolen, guessed, exposed, or otherwise obtained by an unauthorized party.

DOCUMENT CONTROL REGISTER*

For Internal Use Only – Master Document

DOCUMENT TITLE:	DOCUMENT NO.	EFFECTIVE DATE:
Password & Authentication Policy	BA469	Date

DOCUMENT LOCATION: (Where is this document referenced or located; include links to SharePoint or any other locations that are accessible)

REVIEW HISTORY

(Complete log for review only)

REVIEWED YES/NO	REVIEW DATE:	REVIEWED BY:
ANNUAL REVIEW	NEW	VPBA

REVISION HISTORY

(For audit purposes and control tracking)

REASON FOR REVISION: **	REVISED SECTION PAGE# PARAGRAPH:	REVISION #:	REVISION DATE:	APPROVED BY:
NEW			NEW	VPBA