Identification and Authentication (IA) Policy

Policy Title	**Identification and Authentication Policy**
Policy Number	500.007
Effective Date	June 24, 2025
Approved by	• Cydni Sanchez, LOPD, Deputy Chief Public Defender • Theresa Edwards, Deputy Director of Policy and Administration • Matt Bevington, IT Director
Date of Approval	06/24/25
Revision Number	
Purpose of policy	This Policy safeguards LOPD information systems by ensuring that only authorized users and devices can access them. This policy defines how users are identified (e.g., through usernames) and authenticated (e.g., through passwords or multi-factor authentication) before gaining access.
Authority	Per 1.12.20.8-NMAC, all agency IT technical operations shall have documented security operating instructions, management processes, and formal incident management procedures in place that define roles and responsibilities of individuals who operate or use agency IT technical operations and facilities. Per 1.12.20.16 NMAC, to maintain information security, agency must require through published policies and procedures consistent with these rules, that individual accountability shall be maintained at all times.
Definitions	• **Account management:** includes password policies, account lockouts, and account access controls • **Authentication:** the process of verifying that a user or device is who they claim to be (e.g., through passwords, biometrics, or tokens), ensuring that only authorized users can access the LOPD IT system or applications. • **Confidential Data** – Confidential data, if compromised, is likely to result in significant and/or long-term harm to the institution and/or individuals who own the data. It includes, but is not limited to, data that is marked as confidential, data a reasonable person would know is confidential, and data designated as confidential under State or federal laws or regulations. • **Contractor** - A person or company under contract to provide goods or services to an Agency. • **LOPD IT Resource Users** - All LOPD employees, contractors, vendors, consultants, temporary staff, seasonal staff, and any other users of LOPD ITresources. • **Identification:** the process of assigning a unique identifier to a user or device (e.g., username, device ID) • **Identifier**: a unique piece of data used to distinguish one entity from another within a system. It can be a name, a number, a string, or any other data that

Identification and Authentication (IA) Policy

	serves as a label or handle for identification. Identifiers ensure that each user within a system can be uniquely recognized and accessed. • **Multi-factor authentication (MFA):** requires users to provide multiple forms of authentication (e.g., something they know, something they have, something they are) for increased security. • **Privileged account**: account that grants access to resources and capabilities beyond the normal user permissions. These accounts are typically used by administrators, system managers, or other personnel with specific roles needing elevated access for tasks like system administration, security, or data manipulation. • **Non-privileged account**: also known as a standard user account, is a user account that has limited access to system resources and administrative functions. These accounts are designed to follow the principle of least privilege, meaning users only have access to what they need to perform their specific tasks.
Scope	This Policy applies to all LOPD users, devices, and applications that access LOPD's IT infrastructure.
Identifier Management	LOPD identifier management policy is a set of rules and procedures that LOPD IT uses to manage digital identifiers, such as user accounts, access rights, and device IDs. It ensures that these identifiers are unique, secure, and properly managed throughout their lifecycle, from creation to deletion. **<u>Unique User Identifier</u>** Upon request by an LOPD department supervisor, LOPD IT Director shall assign unique user identifiers (e.g., usernames) to each employee and contractor. These identifiers are used for access control to LOPD IT systems. • LOPD IT Director verify the identities of LOPD IT resource users. • LOPD IT Director shall monitor and audit identifiers to ensure each identifier is unique and linked to a specific user. • Shared accounts are prohibited unless explicitly approved by the IT Director with proper audit controls. • System-generated identifiers must be traceable to a person • LOPD IT Director shall grant user access based on the "need to know" principle, limiting access to the minimum required for the LOPD IT resource user's job functions. • LOPD IT Director shall not reuse identifiers.

Identification and Authentication (IA) Policy

	• LOPD IT staff shall manage these identifiers and ensure they are securely stored and protected. • LOPD IT staff shall disable identifiers after 30 days of inactivity. While this is not a current practice of LOPD, we retain this requirement for future consideration. • LOPD IT Director shall revoke LOPD user access to all or selected systems or applications when a supervisor requests or when a user leaves the employ of LOPD, changes their role in LOPD, or violates LOPD security policies.
Authentication Management	The LOPD IT Department shall verify users before establishing a network connection or giving them access to an LOPD system or application. To verify users, the LOPD IT Department shall employ user identifiers, user passwords, and multi-factor authentication (MFA) as outlined above. **Authentication Mechanisms:** All users must authenticate using at least one factor from two of the following categories: • Something you know (password, PIN) • Something you have (security token, mobile authenticator) **Strong Password** • In addition to a unique user identifier, each LOPD IT resource user must establish a strong password. • Strong passwords should have the following characteristics: ✓ Be a minimum of 12 characters in length ✓ Include a CAPITAL letter ✓ Include a lowercase letter ✓ Include at least one number ✓ Include at least one symbol (e.g. #, $, *, !, etc.) ✓ If possible, include a passphrase (e.g., +RockClimbing_18Mountain^Peak) that users can remember and not have to write down. Another possibility is the first letters of a memorable phrase or a meaningful quote. ✓ Not include common dictionary words, usernames, or personal information ✓ Be validated against a blacklist of breached or weak passwords ✓ When the LOPD system user is obtaining system access, the IT system shall first assign the user a temporary password. When the new LOPD IT resource user first connects to the LOPD IT system, the new user must change the temporary password to a permanent password. • Users must update passwords every 60 days. Required password update can also be triggered by: ✓ Indicators of compromise (IOC) ✓ User-requested resets

Identification and Authentication (IA) Policy

	✓ Account recovery processes • Users shall be unable to reuse previous passwords when setting up a new password. • Users must not share passwords with anyone except an LOPD IT staff member. • Users must not send a password via email. • System interfaces must mask password entry and encrypt credentials at rest and in transit **<u>Multifactor Authentication</u>** • For LOPD IT resource users who need to have a privileged IT account or need to have access to confidential or restricted information due to their role or job functions, the LOPD IT Director shall add multifactor authentication as a requirement for user access, in addition to requirement of a unique identifier and a strong password. • Multifactor Authentication (MFA) is required for: ✓ Remote access (VPN, virtual desktops) ✓ Administrative system access ✓ Access to systems housing confidential client data, PII, or regulated records. While this is not a current practice of LOPD, we retain this requirement for future consideration. **<u>Authentication Content Protection</u>** LOPD IT shall protect authentication content from unauthorized disclosure and modification. **<u>Required Re-Authentication</u>** LOPD IT resource users must re-authenticate to access the LOPD systems in the following circumstances: • User logout after five (5) consecutive failed login attempts • After IT system upgrade/update
Incident Management	**Incident Management** is how an organization quickly identifies, responds to, and recovers from unexpected events, such as hacks, system failures, or data leaks, that could harm operations or data. An **incident** is any event that disrupts normal services or threatens the security of systems or information. Incident Management ensures the integrity and security of authentication mechanisms. • Detection and Reporting of Authentication-Related Incidents

Identification and Authentication (IA) Policy

	✓ Any unauthorized access, authentication failure anomaly, account compromise, or repeated login attempts must be classified as a security incident. ✓ Users and system administrators must report suspicious login activities or credential misuse immediately to the designated IT Director in accordance with NMAC 1.12.20.20 (D) and NIST 800-53 IR-4. • Immediate Account Revocation ✓ Upon confirmation of a suspected or actual compromise of user credentials or authentication systems, affected accounts must be disabled or access revoked immediately, per NIST 800-53 AC-2(5) and NMAC 1.12.20.20 (A). ✓ Privileged accounts must be prioritized in the revocation process to minimize risk exposure. • Credential Reset and Forensic Review ✓ All compromised credentials must be reset using secure procedures with identity verification. ✓ A forensic review must be conducted to determine the root cause, access scope, and duration of compromise, supporting NIST 800-61 (Computer Security Incident Handling Guide). • Authentication Log Retention and Review ✓ Authentication and access logs must be retained for at least 90 days and regularly reviewed for anomalies, in compliance with NMAC 1.12.20.22 (A–C). ✓ Logs must include successful and failed login attempts, account lockouts, and password changes. • Incident Notification and Escalation ✓ Incident response procedures must include formal escalation paths, including notification to New Mexico DoIT within mandated timeframes (i.e., within 24 hours of confirmed security incident, per NMAC 1.12.20.18 (A)). ✓ Incidents involving CJIS systems must also follow applicable federal reporting timelines. • Lessons Learned and Policy Updates ✓ Following resolution, the organization shall conduct a "lessons learned" meeting to identify gaps and update the Identification and Authentication Policy if necessary. ✓ Results shall be documented and used to improve training and technical safeguards per NIST 800-53 IR-8 and PL-2.
Policy Review and Update	LOPD IT Director will review, update, and disseminate this policy annually at a minimum, to ensure accuracy, clarity, and completeness.

Identification and Authentication (IA) Policy

Exceptions	Requests for exceptions to this policy shall be reviewed by the LOPD IT Director. The request should specifically state: • The scope of the exception • Justification for granting the exception • The potential impact or risk attendant upon granting the exception • Risk mitigation measures • Time-frame for achieving the minimum compliance level with the policies. The LOPD IT Director shall review the requests and confer with the requestors.
Policy Audit	LOPD IT Department shall track user access and authentication attempts for security analysis and monitoring. Authentication logs must be retained for a minimum of 180 days and be auditable
Roles and Responsibilities	**LOPD IT Director is responsible for:** • Reviewing and approving LOPD access requests. Level of access will be based on **"**need to know" principle, limiting access to the minimum required for the LOPD IT resource user's job functions. • Adding multifactor authentication to access requirements for privileged IT accounts or for LOPD IT resource users who need to access confidential or restricted information. • Reviewing and approving requests to revoke access to LOPD IT resources • Revoking LOPD user access to all or selected systems or applications when a user leaves the employ of LOPD, changes their role in LOPD, or violates LOPD security policies. • Verifying the identities of LOPD IT resource users. • Ensuring identifiers are not reused • Monitoring and auditing identifiers to ensure each identifier is unique and linked to a specific user. • Assigning access tasks to LOPD IT Staff • Reviewing the Identification and Authentication Policy at least once a year. **LOPD IT staff is responsible for:** • Setting up LOPD IT resource users with the specified access. • Disabling identifiers after 30 days of inactivity • Ensuring that LOPD IT Resource Users are uniquely identified and authenticated before they are granted access to LOPD information resources • Managing LOPD IT resource users' identifiers and ensuring they are securely stored and protected.

Identification and Authentication (IA) Policy

Party responsible for implementing policy	Matt Bevington, IT Director