Policy Title	**Access Control Policy**
Policy Number	500.008
Effective Date	06/24/25
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 Access Control Policy establishes a comprehensive and risk-based approach to ensure that only authorized individuals have access to LOPD systems, data, and physical environments.
Authority	• NIST SP 800-83 (Malware Incident Prevention and Handling) • NIST SP 800-30 (Risk Management Guide for Information Technology Systems) • NIST SP 800-53 Rev. 5 Access Control (AC) control family
References	• NIST SP 800-53 Rev. 5 (AC, IA, PE, CA, SC families) • NIST SP 800-83 Rev. 1 • NIST SP 800-30 Rev. 1 • NM DoIT Statewide Security Standards
Scope	This policy applies to all personnel, including employees, interns, volunteers, contractors, and third parties, who access NM LOPD systems, applications, facilities, or data.
Definitions	• Access Control: Mechanism to restrict use of systems and data • RBAC: Role-Based Access Control • MFA: Multi-Factor Authentication • BCDR: Business Continuity and Disaster Recovery • PII: Personally Identifiable Information
Access Control Principles	To protect confidentiality, integrity, and availability of sensitive case files, legal documents, and restricted data, LOPD enforces the following access control principles: • Least Privilege: Access privileges must be limited to the minimum necessary for personnel to perform their duties. This includes: ✓ Restricting write, delete, and administrative capabilities unless explicitly required ✓ Regularly auditing access rights based on job responsibilities and separation of duties • Need-to-Know: Access to case information or protected legal materials must only be granted if directly required for an individual's role or assigned case matter. ✓ Client-attorney confidentiality must be preserved at all times through controlled document access • Role-Based Access Control (RBAC):

Policy Title	Access Control Policy
	✓ Roles must be defined for each functional position (e.g., attorney, paralegal, IT administrator) ✓ Access profiles must be pre-approved and documented ✓ Assignment to a role must be reviewed and approved by the appropriate office administrator. • Access Design Review: ✓ All systems and applications must have documented access matrices mapping roles to permissions. ✓ Access requirements must be reviewed during application development or procurement • Access Lifecycle Controls: ✓ Access rights must be reviewed: o Immediately upon employee departure, role change, or project termination • Best Practices for Law Office Environments: ✓ Ensure separation between criminal, juvenile, and agency civil litigation case repositories through logical segmentation ✓ Restrict shared or group accounts unless technically justified and formally approved ✓ Encrypt all access credentials and apply account lockout after multiple failed login attempts These principles align with NIST SP 800-53 AC-1, AC-2, AC-6, and enforce compliance with NMAC 1.12.20.8(A-B) regarding least privilege and secure system access control implementation.
User Identification and Authentication (AC-2, IA-2)	To ensure accountability, auditability, and protection of client-sensitive legal data, LOPD must implement robust user identification and authentication measures as follows: • Unique User Identification: ✓ Each user must be assigned a unique account identifier. Shared accounts are prohibited. ✓ System-generated identifiers must be traceable to a person ✓ Service accounts must be uniquely identified, tied to system functions, and periodically reviewed. • Authentication Mechanisms: ✓ All users must authenticate using at least one factor from two of the following categories: o Something you know (password, PIN) o Something you have (security token, mobile authenticator) o Something you are (biometric verification) ✓ Multifactor Authentication (MFA) is required for: o Remote access (VPN, virtual desktops)

Policy Title	Access Control Policy
	○ Administrative system access ○ Access to systems housing confidential client data, PII, or regulated records • Password Requirements (NIST SP 800-63B): ✓ Passwords must: ○ Be a minimum of 12 characters in length ○ Include a CAPITAL letter ○ Include lowercase letter ○ Include at least one number ○ Include at least one symbol (e.g. #, $, *, !, etc) ○ Recommendation of a passphrase (e.g., +RockClimbing_18Mountain^Peak) is the best something users can remember and not have to write down ○ Not include common dictionary words, usernames, or personal information ✓ Password expiration automatically expires every 60 days. Expiration is also triggered by: ○ Indicators of compromise (IOC) ○ User-requested resets ○ Account recovery processes ✓ Reuse of previous passwords is prohibited for the last 6 iterations • System and Application Requirements: ✓ Login systems must support account lockout after five (5) consecutive failed login attempts ✓ Authentication logs must be retained for a minimum of 180 days and be auditable ✓ System interfaces must mask password entry and encrypt credentials at rest and in transit • Biometric and Certificate-Based Authentication: ✓ Where biometric or smart card technologies are used, they must: ○ Be compliant with FIPS 201 or equivalent standards ○ Be accompanied by a backup authentication method • Best Practices for Law Office Environments: ✓ Ensure legal teams accessing criminal, civil, or juvenile systems do so via segregated access paths and secure portals These requirements align with NIST SP 800-53 Rev. 5 AC-2 (Account Management), IA-2 (Identification and Authentication), NIST SP 800-63B (Digital Identity Guidelines), and NMAC 1.12.20.16(C) regarding identity validation and secure credential usage.
Account Provisioning and Deprovisioning	To maintain the integrity of system access and prevent unauthorized use, LOPD shall implement rigorous account lifecycle procedures as outlined below: • Onboarding and Access Requests:

Policy Title	Access Control Policy
	✓ Access requests must be initiated using a standardized onboarding form or ticketing workflow ✓ Required approvals include: o When contractors are hired, the department that is hiring the contractor will make the request for approval. o Data/System Owner to confirm access scope and job relevance ✓ The request form must include: o Role-based justification o Start date and anticipated end date (if applicable) o Systems and data to be accessed • Pre-Provisioning Requirements: ✓ Accounts must only be created after the user has: o Completed all required security awareness and acceptable use training. While this is not a current practice of LOPD, we retain this requirement for future consideration. o Signed the LOPD Computer Systems, Internet, Intranet, and Email Usage Policy (NMPD 500-004) o Been assigned an access role under documented RBAC standards ✓ Generic or shared accounts are prohibited • Provisioning Controls: ✓ IT administrators must: o Create accounts with the minimum required privileges o Document accounts in an access control log or directory system o Configure expiration dates for temporary or project-based accounts • Deprovisioning Procedures: ✓ When a user separates from LOPD (voluntarily or involuntarily), their account must be: o Disabled within 24 hours o Documented in the access control system o Reviewed to ensure return of LOPD-issued equipment and credentials ✓ Terminations must be coordinated with HR, IT, and the Data/System Owner ✓ Orphaned accounts must be reviewed monthly and deactivated immediately if unused. (An orphaned account (also called an orphan account) is a user account (employee or vendor) that retains access to applications and systems on a network without an active owner (additionally the account is often not associated with a legitimate, current user). There are many reasons why the original account owner (identity) may be inactive in the system.) While this is not a current practice of LOPD, we retain this requirement for future consideration. • Access Recertification and Review: ✓ All accounts must be:

Policy Title	Access Control Policy
	○ Reviewed quarterly by system owners and the IT Director. While this is not a current practice of LOPD, we retain this requirement for future consideration. ○ Audited against current job roles, project assignments, and organizational changes. While this is not a current practice of LOPD, we retain this requirement for future consideration. ✓ Role-based access lists must be validated and adjusted for promotions, reassignments, or terminations. While this is not a current practice of LOPD, we retain this requirement for future consideration. These procedures align with NIST SP 800-53 Rev. 5 AC-2 (Account Management), AC-5 (Separation of Duties), and AC-6 (Least Privilege) as well as NMAC 1.12.20.16(B) standards for access authorization and lifecycle documentation.
Privileged Account Management (AC-5, AC-6, AC-17)	To protect high-value administrative functions and prevent unauthorized changes to sensitive legal systems, LOPD shall implement strict management of privileged accounts: • Privileged Account Classification: ✓ Privileged accounts include: ○ System administrators ○ Database administrators ○ Network engineers ○ Security engineers ○ Application support teams with elevated rights ○ LOPD Leadership • Account Segregation (does not apply to LOPD Leadership): ✓ Privileged accounts must be: ○ Separate from user accounts used for daily activities ○ Labeled with identifiable prefixes/suffixes (e.g., ADM_jdoe) ○ Logged into only when performing approved administrative functions • Access Authorization and Role Assignment: ✓ Assignment of privileged access must be: ○ Approved by the IT Director and System Owner ○ Justified with a business or technical need • Logging and Monitoring: ✓ All privileged account activity must be: ○ Logged with full audit trails (timestamp, user, actions taken) ○ Monitored by security operations for signs of misuse, anomalies, or escalations. While this is not a current practice of LOPD, we retain this requirement for future consideration. ○ Reviewed at least monthly by the IT Director. While this is not a current practice of LOPD, we retain this requirement for future consideration.

Policy Title	Access Control Policy
	✓ Logs must be: o Retained for at least one year o Protected against unauthorized modification or deletion • Remote Privileged Access Controls: ✓ Remote administrative access must: o Use encrypted communication channels (e.g., VPN, SSH, TLS 1.2+) o Require multi-factor authentication (MFA) o Be limited to pre-approved IP ranges or devices o Be monitored in real time when feasible (e.g., for elevated systems or incident response platforms) While this is not a current practice of LOPD, we retain this requirement for future consideration. • Privileged Access Reviews: ✓ Conduct quarterly access reviews of all privileged accounts, roles, and entitlements ✓ Immediately revoke access upon role change, separation, or completion of a temporary assignment • Best Practices for Legal Office Context: ✓ Ensure administrative accounts cannot access case files or legal systems not associated with their technical function ✓ Require dual authorization or peer-review for critical changes (e.g., firewall modifications, case management database edits) These practices align with NIST SP 800-53 Rev. 5 AC-5 (Separation of Duties), AC-6 (Least Privilege), AC-17 (Remote Access Controls) and satisfy compliance obligations in NMAC 1.12.20.16(E) regarding administrative access and auditability.
Physical Access Control (PE-2, PE-3)	To ensure the confidentiality, integrity, and availability of critical LOPD assets, physical access controls shall be implemented in all LOPD security zones (facilities and locations housing sensitive systems, case records, or infrastructure). These requirements also apply to alternate facilities (if used). Access levels include: • Secured: applies to LOPD personnel, contractors, and vendors. These personnel have building access as needed to fulfill their job duties. • Visitor: applies to persons who are not employed or contracted with LOPD who have no secured building access and must be escorted at all times when in secured LOPD areas. Secured Building Access Requirement • Secured Identification and Entry Requirements: ✓ Access to secured LOPD buildings or spaces must require one or more of the following: o Agency-issued ID badge

Policy Title	Access Control Policy
	○ Biometric authentication (e.g., fingerprint or facial recognition) ○ Proximity-based keycard or smart card system ✓ Physical credentials must be: ○ Issued only after verification of employment or contract authorization ○ Deactivated immediately upon employee separation ○ Reviewed and reconciled quarterly • Server Rooms and Sensitive Storage Areas: ✓ Server Rooms and Sensitive Storage Areas include: ○ Data centers ○ On-site server closets ○ Secure backup storage vaults • Confidential records rooms must be restricted to authorized personnel only • Visitor Access: ✓ Visitors must: ○ Be signed in and escorted at all times • Physical Security Reviews: ✓ Physical access controls must be reviewed: ○ Annually by the IT Director and Safety and Loss Control Coordinator ○ After significant renovations, relocation, or incidents ✓ Doors, locks, and readers must be tested quarterly • Best Practices for Legal Environments: ✓ Keep physical records in fire-resistant, locked file cabinets or safes ✓ Segregate access to criminal, juvenile, and agency civil litigation record archives ✓ Ensure that no client-related paper records are left unsecured in shared or open office spaces ✓ Individuals with authorized access are not permitted to allow unknown or unauthorized persons to access Secured Areas, including by way of Tailgating. ✓ Employees must notify their LOPD manager or supervisor when they encounter unescorted visitors ✓ Individuals with Access Control Badges that have been lost or stolen, or are suspected of being lost or stolen, are required to report the loss/theft to the Office Administrator or manager immediately. ✓ Display screens that handle sensitive or confidential information must be positioned to not be viewable by unauthorized individuals (e.g., from public windows, doors with windows, waiting areas, etc.). These measures align with NIST SP 800-53 Rev. 5 PE-2 (Physical Access Authorizations) and PE-3 (Physical Access Control) and meet physical access policy requirements in NMAC 1.12.20.16(A).

Policy Title	Access Control Policy
Access Reviews and Audits (CA-7, AC-2(4))	To maintain least privilege and mitigate risks associated with unauthorized access, LOPD must implement formal access review and auditing procedures as follows: • Quarterly Access Reviews: ✓ Conduct quarterly reviews of all user accounts, permissions, and roles across all major systems ✓ Reviews must be: o Conducted by system owners in coordination with the IT Director or their designee o Documented using standardized access review templates o Approved by management and retained for no less than one year • Triggers for Role-Based Access Updates: ✓ Access must be reviewed and updated upon: o Change in role, responsibilities, or department o Completion or termination of a project or case o User separation from LOPD (voluntary or involuntary) o Detection of suspicious activity or policy violation • Internal Security Assessments: ✓ Access controls and account configurations must be: o Audited during all internal security assessments or audits (at least annually) o Aligned with user access logs and incident reports o Evaluated for over-provisioning, orphaned accounts, and access anomalies • Key Metrics and Reporting: ✓ Review outcomes must be summarized and submitted to the IT Director or their designee, including: o Number of accounts reviewed o Number of permissions modified or revoked o Remediation actions taken o Recertification status of privileged accounts • Law Office-Specific Best Practices: ✓ Ensure that access to case management systems is revalidated upon reassignment or case closure ✓ Limit access to sealed or expunged case files to court-approved personnel only ✓ Use automated reporting tools to track excessive access rights to sensitive case or evidence repositories These requirements support NIST SP 800-53 Rev. 5 AC-2(4) (Account Review) and CA-7 (Continuous Monitoring), and help fulfill auditability standards in NMAC 1.12.20.16(F).

Policy Title	Access Control Policy
Network and System Access (SC-7, AC-19)	To protect the confidentiality and integrity of LOPD systems and data, all access to internal and external networks must be governed by secure, role-based controls and segmentation. The following practices apply: • Secure Connection Requirements: ✓ All remote access to LOPD systems must: o Be established via an encrypted Virtual Private Network (VPN) o Require multi-factor authentication (MFA) o Utilize endpoint validation checks prior to connection (e.g., antivirus status, OS patch level) • Internal Segmentation and Isolation: ✓ Network segmentation must be enforced to: o Separate public-facing services from internal business applications o Limit lateral movement in the event of a compromise o Create secure zones for high-risk or regulated data (e.g., PII, legal records) • Guest and Temporary Access: ✓ Any temporary or guest access (e.g., contractors, consultants, interns): o Must be formally requested, documented, and approved by the System Owner and IT Director or their designee o Shall be time-bound, with default expiration settings o Must be restricted to isolated VLANs with no access to case management systems, file shares, or sensitive resources unless specifically required and approved • Access Restrictions and Controls: ✓ All access must: o Be enforced through network access control (NAC) or equivalent solutions o Include session timeout and lockout features after periods of inactivity o Be logged and monitored for anomaly detection • Law Office-Specific Best Practices: ✓ Access to internal legal databases should be restricted by case type, client assignment, or geographic location as applicable ✓ Internal firewall rules should prevent unapproved traffic to or from external jurisdictions without review by the IT Security team These requirements align with NIST SP 800-53 Rev. 5 SC-7 (Boundary Protection) and AC-19 (Access Control for Mobile Devices) and help meet state security standards defined in NMAC 1.12.20.8(F) and 1.12.20.16(C).

Malware and Risk Considerations (NIST SP 800-83, 800-30)	To minimize threats related to unauthorized access and malicious software, LOPD must implement layered controls and maintain continuous awareness of access-related risk factors: • Malware Prevention through Access Controls: ✓ Enforce technical controls that: o Prohibit the installation of unauthorized or unlicensed software o Block execution of unverified code, scripts, and macros from unknown sources o Restrict the use of removable media (e.g., USB drives, external hard drives) to agency-approved, encrypted devices only ✓ Monitor remote sessions for: o Malware activity and data exfiltration behavior. While this is not a current practice of LOPD, we retain this requirement for future consideration. o Abnormal login patterns or elevated privilege requests. While this is not a current practice of LOPD, we retain this requirement for future consideration. ✓ Implement endpoint protection tools that: o Integrate with access control systems o Provide real-time threat detection and quarantine capabilities • Risk Assessments for Access Controls: ✓ Conduct formal access-related risk assessments: o Annually, or following a significant system change, migration, or security incident. While this is not a current practice of LOPD, we retain this requirement for future consideration. o In accordance with NIST SP 800-30 methodology (identify, assess, and prioritize risks). While this is not a current practice of LOPD, we retain this requirement for future consideration. o Focused on identifying potential threat vectors impacting: ▪ Authentication mechanisms. While this is not a current practice of LOPD, we retain this requirement for future consideration. ▪ Role-based access assignments. While this is not a current practice of LOPD, we retain this requirement for future consideration. ▪ Remote and mobile access points ✓ Document results in the LOPD Risk Register, including: o Identified vulnerabilities. While this is not a current practice of LOPD, we retain this requirement for future consideration. o Associated threat actors (e.g., malware, insider threats, third-party compromise). While this is not a current practice of LOPD, we retain this requirement for future consideration. o Mitigation strategies and implementation timelines. While this is not a current practice of LOPD, we retain this requirement for future consideration.

Policy Title	**Access Control Policy**
	✓ Review findings with the IT Director and relevant system owners. While this is not a current practice of LOPD, we retain this requirement for future consideration. • Law Office-Specific Best Practices: ✓ Ensure all court case documents are scanned using malware-scanning software before ingestion into internal systems ✓ Prevent installation of legal research tools or plug-ins unless vetted and authorized ✓ Require multi-party review of any privileged-access change requests involving external litigation systems or digital evidence repositories These practices align with NIST SP 800-83 (Malware Protection for Information Systems) and NIST SP 800-30 (Guide for Conducting Risk Assessments), and are consistent with state expectations under NMAC 1.12.20.8(C), (D), and (F).
Exceptions	Any exception to this policy must be documented, approved by the IT Director, and subject to periodic review.
Roles and Responsibilities	• IT Director and/or Chief Public Defender: Policy oversight, approval of exceptions • System Owners: Authorization and periodic review of user access • IT Director: Policy implementation and audit coordination • IT Administrators: Provisioning, monitoring, and revocation of accounts • All Users: Compliance with access protocols and reporting of suspicious activity
Party responsible for implementing policy	Matt Bevington, IT Director