Law Offices of New Mexico Public Defender
Policy and Procedure

Policy Title	**LOPD Configuration Management Policy**
Policy Number	500.006
Effective Date	05/20/25
Approved by	• Adrianne Turner, LOPD, General Counsel • Cydni Sanchez, LOPD, Deputy Chief Public Defender • Theresa Edwards, Deputy Director of Policy and Administration • Matt Bevington, IT Director
Date of Approval	05/20/25
Revision Number	
Purpose of policy	Provide a structured approach to managing and controlling IT assets, ensuring they are consistently configured and documented. This approach helps maintain system integrity, facilitates change management, and supports compliance efforts
Definitions	• Baseline Configuration: the standard configurations for systems and applications, serving as a reference point for future changes. It can include various aspects of a system or project, not just individual configuration items. • Configuration item: a fundamental, identifiable, and manageable component of a system, whether hardware, software, or both, that is managed as a single entity for change management and configuration management purposes. • Information Technology (IT) System: an interconnected set of components, including hardware, software, data, people, and processes, that work together to collect, store, process, and transmit data and digital information to support decision-making and operations.
Authority	NMAC 1.12.20.8 (2010) provides "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."
References	This policy references the LOPD Change Management Policy, dated April 2025
Scope	The Configuration Management Policy applies to all LOPD IT systems and configuration items used in LOPD IT systems. These systems include but are not limited to: • Network**:** ✓ Physical network infrastructure (routers, switches, cables, etc.) ✓ Servers providing network services, data storage, other core infrastructure functions ✓ Related software (firewalls, VPNs, etc.) • User devices, software, applications, peripherals, and helpdesk support: ✓ Workstations ✓ Operating systems on devices (Windows) ✓ Applications: Office 2016, Office 2021, Microsoft 365, Smart Deploy Adobe, ZOOM, Snagit, FTR, VLC Player, ESET, Halcyon, VNC ✓ Mobile devices ✓ Peripherals used by staff (printers, mice, keyboards, monitors, etc.) ✓ Telephone equipment

	• Security: ✓ Firewalls: Sonicwall firewall ✓ Antivirus software ✓ Intrusion detection systems ✓ Other tools to protect systems from cyber threats: Cisco Umbrella, Lumu web security, ESET, Halcyion, Sentinal One, end point security, Proofpoint email security with URL defense. DUO 2FA security, and Sonicwall SMA VPN with security end point control. • Services: ✓ Email ✓ Web hosting ✓ Database services ✓ Cloud-based services, including Barcloud Inventory Control application controlled by ASAP software • Documentation: stored on IT only shared drive ✓ Policies, procedures ✓ User guides, including Microsoft One Note knowledge base document ✓ Other documentation related to the IT system.
Configuration Items	LOPD IT System includes the following configuration items: • Network**:** ✓ Physical network infrastructure (routers, switches, cables, etc.) ✓ Servers providing network services, data storage, other core infrastructure functions ✓ Related software (firewalls, VPNs, etc.) • User devices, software, applications, peripherals, and helpdesk support: ✓ Workstations ✓ Operating systems on devices (Windows) ✓ Applications: Office 2016, Office 2021, Microsoft 365, Smart Deploy, Adobe, ZOOM, Snagit, FTR, VLC Player, ESET, Halcyon, VNC, Sentinel One ✓ Mobile devices ✓ Peripherals used by staff (printers, mice, keyboards, monitors, etc.) ✓ Telephone equipment • Security: ✓ Firewalls: Sonicwall firewall ✓ Antivirus software ✓ Intrusion detection systems ✓ Other tools to protect systems from cyber threats: Cisco Umbrella, Lumu web security, ESET, Halcyon, Sentinel One, end point security, Proofpoint email security with URL defense. DUO 2FA security, and Sonicwall SMA VPN with security end point control. • Services: ✓ Email ✓ Web hosting

	✓ Database services ✓ Cloud-based services, including Barcloud Inventory Control web-hosted application controlled by ASAP software • Documentation: stored on IT only shared drive ✓ Policies, procedures ✓ User guides, including Microsoft One Note knowledge base document ✓ Other documentation related to the IT system.
Policy	Configuration Item Identification: LOPD IT Department shall: • Identify LOPD IT Configuration items by selecting which IT system items are critical for the system's functionality and require individual management • Document each configuration item in the IT Inventory described below. • Document and map how the configuration item systems are organized and how they work together. Baseline Configuration: • LOPD IT Department shall develop, document, and maintain under configuration control a current baseline configuration of LOPD Configuration Items. This baseline will cover all LOPD IT system configuration items plus any desired additional aspects of a system or project. The baseline configuration shall be based on the Center for Internet Security (CIS) Configuration baselines for: ✓ Cloud Providers: ○ Microsoft 365 ✓ Desktop Software: ○ Microsoft Exchange Server ○ Microsoft Office 2016 ○ ZOOM ○ Microsoft Web Browser (Edge) ✓ Mobile Devices: ○ Google Android ✓ Operating Systems ○ Microsoft Windows Desktop 10 Enterprise, Release 1703 ○ Microsoft Windows Desktop 11 Enterprise ○ Microsoft Windows Server 2019 ○ Microsoft Windows Server 2022 ✓ Server Software ○ Microsoft IIS Summaries of the CIS baseline documents are stored in \\qumulo1\abqmembsvr\abqbu\Apps$\Install\IT Docs\IT App Guides

- LOPD IT Department shall develop additional baseline documents based on user documentation for
  - ✓ Smart Deploy
  - ✓ DUO 2FA security
  - ✓ Sentinel One
  - ✓ Halcyon
  - ✓ Sonicwall SMA VPN

These additional baseline documents are stored in \\qumulo1\abqmembsvr\abqbu\Apps$\Install\IT Docs\IT App Guides

- LOPD IT Department shall:
  - ✓ Review and update the baseline configuration of LOPD Configuration Items at least once a year and will ensure that it is consistent with LOPD Security Configuration Checklist.
  - ✓ Review and update the baseline configuration of the information system when required as a result of a security breach or other unexpected system failure and as an integral part of information system component installations and upgrades.
  - ✓ Retain one previous version of baseline configurations of information systems to support rollback.
  - ✓ The Baseline Configuration Document shall be controlled by the IT Director, stored on the IT Network Drive, and accessible to all IT staff.

<u>Newly Acquired OTS Product Configuration</u>
As part of the implementation of newly acquired off-the-shelf (OTS) products, LOPD IT Department shall:
Review product configuration to evaluate whether:

- It is consistent with LOPD baseline configuration
- It is consistent with LOPD Security Configuration Checklist
- It is the most restrictive mode consistent with operational requirements.
- Identify, document, review, and, if appropriate, approve any deviations from established baseline configuration settings for LOPD information system components based on LOPD operational requirements.
- Complete the configuration.
- Monitor and control changes to the configuration settings in accordance with change management policies and procedures.

<u>Configuration Change Control</u>
LOPD IT Department shall:

- Review proposed configuration changes to the information system following the LOPD Change Management Policy with explicit consideration for security impact analyses, including consistency with LOPD Security Configuration Checklist.

- After detailed review, approve or disapprove proposed changes.
- Document configuration change decisions associated with the information system in the LOPD Change Management Log.
- Test, validate, and document changes to the information system before implementing the changes on the operational system.
- Work with approved implementation teams to implement approved configuration-controlled changes to the information system.
- Retain records of configuration-controlled changes to the information system for two years from date of change.
- Audit and review Change Management Process at least yearly
- Coordinate and provide oversight for configuration change control activities through the Change Management Board as described in the LOPD Change Management Policy.

<u>Information System Component Inventory:</u>

LOPD IT Department shall:

- Ensure that the BARCLOUD Inventory System fulfills the inventory requirements below:
- Reflects the current information system accurately.
- Includes the degree of granularity deemed necessary for tracking and reporting.
- Includes information deemed necessary to achieve effective information system component accountability, including biannual audits by LOPD Finance Department.
- Review and update the information system component inventory at least every six months or as required by audits.
- Update the inventory of information system components as an integral part of component installations, removals, and information system updates. Barcloud software fulfills this function.
- Determine and record end-of-life for inventory devices and follow LOPD and State of New Mexico approved practices to destroy and recycle devices.
- Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system. Halcyon and Sentinel One software supports this effort.
- Take the following actions when unauthorized components are detected:
- Disable network access by such components, or
- Isolate the components and notify the IT Director.
- Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

	Software Usage Restrictions LOPD IT Department shall: • Use software and associated documentation in accordance with contract agreements and copyright laws. • Track the use of software and associated documentation protected by quantity licenses to control copying and distribution. • Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. User-Installed Software • No user at LOPD shall install user software without approval by LOPD IT Director. • LOPD IT Department shall enforce this policy through controlling privileged access and blocking the execution of non-approved software.
Change Management	The policy and procedure for managing and controlling changes to configuration items, including change requests, approvals, and rollback procedures is contained in Information Technology Policy 500.005 LOPD Change Management Policy
Configuration Status Accounting	LOPD IT Department shall document changes in configuration by updating the Configuration Item Baseline Configuration Document at least once a year based on changes documented in the Change Management Process.
Configuration Verification and Audit	At least once a year, LOPD IT Department shall audit configuration items by: 1. Gathering documentation 2. Reviewing the IT environment, including how the CIs are related 3. Conducting interviews of key stakeholders 4. Confirming that the CIs actually exist 5. Validating configuration records 6. Evaluating the effectiveness of change management and documentation 7. Identifying discrepancies, including unnecessary and/or non-secure functions, ports, protocols, and services and software programs not authorized to execute on LOPD information systems or prohibited by LOPD security policies. 8. Documenting findings 9. Taking corrective action by adjusting the configuration database or the configuration item to ensure consistency or by disabling functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure or by prohibiting the execution of these unauthorized or prohibited software programs. All system changes must be approved through Change Requests. At least once every two years, 3rd party security consultant shall perform a security penetration test and general security audit on LOPD IT systems.
Roles and Responsibilities	LOPD IT Configuration Manager is responsible for: • Defining the scope and plan for LOPD configuration management • Maintaining the configuration baseline

	• Developing and improving configuration management processes • Identifying and documenting configuration items (CIs) • Maintaining accurate records of CIs in LOPD Inventory • Verifying that configuration meets requirements and standards • Conducting audits to ensure that configuration meets requirements and standards • Managing the Configuration Management Database (CMDB), which includes Configuration baseline, change management documentation, and audit documentation, to ensure data accuracy and consistency • Collaborating with all IT teams to enforce configuration management practices. • Creating and maintaining documentation for tools used to support configuration management. • Providing user support and troubleshooting issues with the relevant configuration management software. LOPD IT Configuration Librarian is responsible for: • Storing and safeguarding all master copies of software and documentation. • Ensuring the integrity and traceability of the configuration throughout the project's life cycle.
Party responsible for implementing policy	Matt Bevington, IT Director