Law Office of New Mexico Public Defender
Policy and Procedure

Policy Title	IT Change Management
Policy Number	Information Technology 500.005
Effective Date	April 3, 2025
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	April 3, 2025
Revision Number	
Purpose of policy	- To ensure that impact and cost of all IT changes are assessed - To ensure that IT changes are coordinated - To ensure that IT changes are documented
Definitions	- Major LOPD IT systems: All systems pertaining to storage and use of production data - IT changes: Updates and system operational changes (such as patches) - Configuration Management: guidelines in the Configuration Management Policy regarding baseline standards for how a system should be configured, version control system for managing different versions of system configuration files and code, and documentation of configuration items.
Scope	This policy applies to all IT changes requested to major IT systems at the Law Office of New Mexico Public Defender (LOPD). It does NOT apply to changes made to individual computers (made by Help Desk)
Change Policy	LOPD staff members who wish to make a major change to a major LOPD IT system must follow the change procedure stated below. All major changes to major LOPD IT systems must fulfill the guidelines stated in the Configuration Management Policy.

Law Office of New Mexico Public Defender
Policy and Procedure

Policy Title	IT Change Management

Procedure	1. Change Requestor: Identify and assess change needed.
	2. Change Requestor: Complete Change Request Form and Change Risk Assessment Form.
	3. Change Requestor: Submit Change Request Form and Change Risk Assessment Form to Change Manager.
	4. Change Manager: Log Change Request.
	5. Change Manager: Review Change Request and Risk Assessment with stakeholders who will be affected by the change, revise Change Request and Risk Assessment as needed.
	6. Submit revised Change Request Form and Risk Assessment Form to Change Request Board
	7. Change Request Board: Assess Change Request and Risk Assessment. If the change has security implications, independent security personnel must be involved in the change assessment.
	8. Change Request Board: Approve, reject, or request revision of Change Request; and inform Change Requestor of decision.
	9. If Change Request Board request revision to Change Request Form:
	   a. Change Requestor: Make changes to Change Request Form as requested by Change Request Board, send documents to Change Manager
	   b. Change Manager: Log revised Change Request, submit Change Request Form and Change Risk Assessment Form to Change Request Board
	   c. Change Request Board: Review revised Change Request.
	   d. Change Request Board: Approve or reject revised Change Request and inform Change Requestor and Change Manager of decision.
	10. Change Requestor (with assistance from Implementation Staff): Execute the change.
	11. Change Manager, Change Requestor and other needed stakeholders (Change Request Board, users, etc.) assess the change made.
	12. Change Requestor: Complete Change Completion Form and submit to Change Manager.
	13. Change Manager: Log Change Completion Form.

Policy Title	IT Change Management

Roles and Responsibilities	• Change Manager is responsible for:
	  ✓ Defining the logging requirements for all change-related activities, including who made the change, when it was made, what was changed, whether risk was assessed.
	  ✓ Ensuring that audit trails are enabled and regularly reviewed.
	  ✓ Developing and defining expedited process for emergency changes, including authorization and documentation needed
	  ✓ Organizing, controlling, and coordinating Change Request Board
	  ✓ Logging Change Requests
	  ✓ Ensuring all approvals completed before implementation
	  ✓ Working with Change Requestor to assess change after implementation
	  ✓ Logging changes made, success/failure of change, reasons for change success/failure
	  ✓ Logging Change Completion Forms
	  ✓ Reviewing and revising policy at the beginning of each fiscal year.
	  ✓ Archiving documents
	• Requestor is responsible for:
	  ✓ Identifying the change needed
	  ✓ Assessing the change for its cost/benefit, its impact, how it will be implemented
	  ✓ Assessing the risk posed by the change and completing the Change Risk Assessment Form
	  ✓ Working with implementation team to determine process to make change, including ensuring that Configuration Guidelines are fulfilled.
	  ✓ Having a back-out plan in case the change fails or causes issues
	  ✓ Completing and submitting the Change Request Form and Change Risk Assessment Form
	  ✓ Implementing change
	  ✓ Ensuring appropriate testing (unit testing, integration testing, user acceptance testing, etc.) is completed
	  ✓ Assessing the change's potential impact on security
	  ✓ Validating change in a test environment before deploying changes to production
	  ✓ Completing and submitting the Change Completion Form
	• Change Management Board is responsible for:
	  ✓ Reviewing Change Requests at least monthly
	  ✓ Ensuring that LOPD security policies and standards are followed. The independent security personnel who serves on the Change Management Board will be responsible for this requirement.
	  ✓ Determining and communicating the committee's response to the change: Approve, Reject, Require change be revised (e.g. scheduled later, implementation plan changed, etc.)

Party responsible for implementing policy	Matt Bevington, IT Director