

LAW ENFORCEMENT mDL TOOLKIT
DOC-08

Training Plan Framework

Curriculum Outline, Delivery Formats, and Competency Standards for Agency
mDL Training

Audience	Training Officers, Field Training Officers, Supervisors, Command Staff
Purpose	Provides a structured framework for developing and delivering agency-wide mDL training programs, including audience-specific curriculum outlines, recommended delivery formats, competency standards, and a train-the-trainer model.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Customize Before Use

This document provides a framework, not a finished training program. Each agency must adapt this content to reflect its specific reader application, CAD/FBR integration setup, applicable state law, and agency policy. Before finalizing training content, confirm all technical procedures with your reader vendor and all legal content with agency counsel.

Training Program Overview

A complete agency mDL training program addresses four distinct audiences with different informational needs:

Audience	Primary Need	Training Modules
Patrol Officers	How to use the reader in the field; what to do when it doesn't work	Modules 1–5 (full curriculum)
Supervisors / Sergeants	Officer oversight, policy interpretation, and escalation procedures	Modules 1–5 plus Supervisor Supplement
Technology / IT Staff	Device deployment, integration management, CJIS compliance	Modules 1, 3, and IT Technical Supplement
Command Staff	Strategic context, legal landscape, and policy requirements	Module 1 and Executive Briefing (30 min)

Training Curriculum — Module Outlines

Module 1: What Is an mDL? (30 min — All Personnel)

This foundational module is required for all agency personnel. It provides the conceptual framework all other modules build on.

- **Learning Objectives:** Personnel will be able to explain what an mDL is, how it differs from a photo of a license, and why ISO/IEC 18013-5 compliance matters.
- What mDL is — and is not (not a photo, not a barcode scan, not a visual display)
- The three parties: Holder, Issuing Authority, and Verifier
- How cryptographic signing works in plain language (DMV signs the data; reader checks the signature)
- Overview of mDL wallet implementations
- Current state, province, and territory adoption — which jurisdictions have mDLs your officers will encounter
- Legal status in your jurisdiction — what the law says about accepting mDLs

Module 2: Field Verification — Using the Reader (60 min — Patrol + Supervisors)

Hands-on skill development module. Must include practical demonstration and scenario-based exercise using the agency's actual reader application.

- **Learning Objectives:** Officers will be able to successfully initiate and complete an mDL verification session using the agency's reader app, compare the returned photo to the holder, and interpret the displayed validity information.
- Opening and preparing the reader application
- QR code engagement — step-by-step demonstration
- NFC engagement — step-by-step demonstration
- Interpreting the holder's consent screen — what the holder sees
- Reading the reader's output — what valid looks like, what an alert looks like
- Photo comparison — how to compare the mDL portrait to the person in front of you
- Hands-on exercise: Each officer completes a minimum of 3 successful verification sessions

Module 3: Workflow Integration — Data Use and Reporting (45 min — Patrol + Supervisors, Technical Support)

Focuses on the downstream use of mDL data — the primary value driver of the technology.

- **Learning Objectives:** Officers will be able to transfer mDL data to their CAD/FBR system and confirm auto-population of reports, citations, and query fields.
- How mDL data flows to your agency's specific CAD/FBR system
- Confirming auto-population of report and citation fields
- Submitting a CIC/NCIC query using mDL-sourced DL number
- e-Citation completion using mDL data
- Crash report and arrest report field population
- Hands-on exercise: Complete a simulated traffic stop from mDL scan through e-citation issuance

Module 4: Failure Scenarios and Fallback Procedures (30 min — Patrol + Supervisors)

Prepares officers for real-world conditions where mDL verification does not work as expected.

- **Learning Objectives:** Officers will correctly identify and apply the appropriate response for every common failure scenario, including applicable legal obligations under state law and agency policy.
- Holder's device has no battery or is damaged — request physical credential; follow agency procedures and applicable state law
- Reader cannot establish a session — request physical credential; report failure to technology contact

- Holder declines consent — request physical credential; follow standard no-ID procedures if no credential is produced
- Reader displays authentication failure or warning — do not treat as valid; follow agency policy
- Out-of-state or non-ISO/IEC 18013-5 digital credentials — reader may not authenticate; request physical credential
- Holder claims to have an mDL but app is not working — request physical credential; follow agency procedures
- Scenario exercise: Practice each failure scenario with appropriate response

Module 5: Legal, Privacy, and Policy (30 min — Patrol + Supervisors)

Ensures officers understand their legal obligations and the privacy principles that govern mDL transactions.

- **Learning Objectives:** Officers will correctly state agency policy on data minimization, data retention, physical credential requirements, and applicable state law obligations.
- State/Provincial law on mDL acceptance in your jurisdiction
- Physical credential requirement — drivers are still required to carry physical licenses in most jurisdictions
- Selective disclosure — request only necessary data elements for the specific encounter
- Do not handle the holder's device
- Do not examine phone contents beyond mDL session initiation
- How mDL transaction data is retained (per agency policy)
- Reporting reader failures or policy concerns

Supervisor Supplement (45 min — Supervisors / Sergeants Only)

This supplement is required for all supervisory personnel in addition to Modules 1–5. It equips supervisors to oversee officer mDL activity, interpret policy, manage exceptions, and support the agency's ongoing deployment.

- **Learning Objectives:** Supervisors will be able to evaluate officer competency in mDL verification, apply agency policy to field exceptions, manage complaints, and serve as the first point of escalation for legal and technology issues.

Evaluating Officer Performance

- How to observe and assess officer proficiency in QR and NFC engagement
- Common officer errors: failing to confirm auto-population, skipping photo comparison, mishandling authentication failures
- Competency standards for field clearance — what passing looks like (see Competency Standards section)
- Remediation process for officers who do not meet competency standards

Policy Interpretation and Exceptions

- Applying agency data minimization policy to non-routine encounters (e.g., arrest, DUI investigation, crash)
- Supervising officer response when a holder declines consent — when to escalate
- Handling disputes at point of contact regarding mDL validity or officer authority to require a physical credential
- Jurisdiction-specific legal requirements — when state law mandates acceptance and when it does not

Complaint Handling and Escalation

- Responding to officer complaints about reader equipment or software failures
- Responding to public complaints related to mDL verification encounters
- Escalation path for unresolved legal or policy questions — agency legal advisor, state DMV liaison
- Escalation path for technology failures — agency IT/technology point of contact, vendor support

Ongoing Deployment Responsibilities

- Ensuring assigned officers maintain current training and recertification status
- Communicating policy updates, state law changes, and new reader capabilities to the team via roll call or briefings
- Monitoring for patterns of reader failure or officer non-compliance and reporting to command

Executive Briefing (30 min — Command Staff Only)

This briefing is designed for chiefs, sheriffs, deputy chiefs, and other command-level personnel. It does not require hands-on equipment training. The goal is to ensure command staff can make informed decisions about mDL deployment, respond to policy and legal questions, and provide effective leadership for the agency's adoption of this technology.

- **Learning Objectives:** Command staff will be able to describe the strategic value of mDL technology, articulate the agency's legal authority and obligations, and identify the key decisions required for successful deployment.

The mDL Landscape and Strategic Context

- What an mDL is and why it matters for law enforcement — the shift from physical to digital credentials
- Current national deployment status: which states have active mDL programs and the pace of adoption
- Why agencies that wait will be less prepared: legislative trends and officer encounter rates

- The core operational benefit: mDL data flowing directly into citations, crash reports, and queries — reduced errors, faster stops

Legal and Policy Obligations

- Your jurisdiction's current legal posture on mDL acceptance — mandatory, permissive, or silent
- Physical credential requirements — what the law currently says in your state
- Officer authority and limitations when interacting with mDL holders
- Data retention and privacy obligations — what your agency must have in policy before deploying
- CJIS Security Policy compliance — vendor and system requirements

Deployment Decisions for Command

- Procurement pathway: immediate deployment vs. integrated long-term solution — tradeoffs and timeline
- Funding options: JAG, FMCSA, NHTSA 405(c), and cooperative purchasing vehicles
- Policy development requirements before go-live: data retention, officer authority, acceptable use
- Training rollout strategy: train-the-trainer model, LMS integration, and competency standards
- Metrics and accountability: how to measure successful deployment and officer readiness

Questions for Command to Resolve Before Deployment

- Has legal counsel reviewed applicable state law and confirmed officer authority to accept mDLs?
- Has a data retention policy been adopted covering mDL transaction data?
- Has the agency selected a reader solution with a documented integration path to CAD/FBR?
- Has a vendor CJIS Information Security Agreement been executed?
- Is a training and competency certification process in place before officers are deployed with readers?

Reference for Command Staff

For full detail on any of the topics above, direct command staff to the relevant toolkit documents: DOC-01 (Standards Overview), DOC-05 (Procurement), DOC-06 (Funding), and DOC-07 (Legal & Privacy Considerations).

Delivery Format Recommendations

Format	Best Used For	Notes
In-Person / Hands-On	Modules 2, 3, 4 — skill development requiring practice with actual hardware	Must use the agency's actual reader app and CAD/FBR system — no generic demos
Online / Self-Paced (LMS)	Module 1 initial delivery; Module 5 annual refresher	Build into agency LMS for annual recertification tracking
Roll Call Training	Policy updates, state law changes, new reader capabilities	Keep to 10–15 minutes; issue written roll call handout
Quick Reference Card	Field reference for engagement steps and failure procedures	Laminated card for vest/belt/dash; QR code to refresher video
Video Demonstration	Module 2 walkthrough; failure scenario reference	Short-form (5–10 min); hosted on agency intranet or LMS
Briefing / Presentation	Executive Briefing for command staff	30 min; slide-supported; delivered by training officer or agency technology lead
Train-the-Trainer	Multiplying instructor capacity for agency-wide rollout	Certify 1 trainer per 20–30 officers; require annual recertification

Competency Standards

Officers should be assessed on the following competencies before being cleared to use mDL reader technology in the field:

- **Knowledge:** Can correctly explain what an mDL is, how it is verified, and what the reader output means.
- **Skill — QR Engagement:** Successfully completes QR-initiated mDL verification session with no coaching in at least 3 of 3 attempts.
- **Skill — NFC Engagement:** Successfully completes NFC-initiated mDL verification session with no coaching in at least 3 of 3 attempts.
- **Skill — Data Integration:** Can correctly transfer mDL data to CAD/FBR system and confirm report field population.
- **Judgment — Failure Scenarios:** Correctly identifies appropriate response — including applicable legal obligations — for each of 5 presented failure scenarios without prompting.
- **Policy:** Can correctly state agency policy on data minimization, physical credential requirements, and holder consent.

Related Toolkit Documents

- **DOC-01:** Standards Overview — foundational mDL technology content for Module 1

- **DOC-04:** Operational Workflows — step-by-step field procedures that Modules 2, 3, and 4 must cover
- **DOC-05:** Procurement Considerations & Strategy — deployment decision content for the Executive Briefing
- **DOC-06:** Funding Strategies & Opportunities — funding content for the Executive Briefing
- **DOC-07:** Legal & Privacy Considerations — legal content for Module 5 and the Executive Briefing
- **DOC-09:** mDL Officer How-To Guide — field reference to distribute to officers on completion of Module 2
- **DOC-10:** mDL FAQs for Law Enforcement — supplementary reading for officers completing initial training