CERTIFIED LAW ENFORCEMENT RECORDS MANAGER (CLERM)

GUIDE TO CERTIFICATION

TABLE OF CONTENTS

GUIDE TO CERTIFICATION

Purpose and Use of this Guide

This guide defines the essential knowledge required of personnel working in or preparing for law enforcement records management supervisory or management positions who seek certification as a Certified Law Enforcement Records Manager (CLERM). It serves as the foundational framework for the CLERM certification program offered by the Institute for Public Safety Records Management (IPSRM), and outlines consistent national standards while recognizing that records professionals must also comply with state and local laws, ordinances, and regulations.

This Guide is Designed to:

- Define the scope of professional law enforcement records management supervision and management;
- Define core competencies for records management performance in public safety;
- Support training, certification, and career development;
- Promote compliance, quality control, modernization, and professionalism;
- Elevate the recognition and value of records management roles in public safety.

Overview and Context

Law enforcement records professionals are custodians of various types of operational and administrative records, some of which involve sensitive, consequential, and legally significant information produced by government agencies. Their work directly impacts public safety operations, individual rights, court proceedings, crime reporting accuracy, transparency, and public trust.

A central tenet of records management in public safety is establishing policy, procedure, training, and organizational culture which emphasizes quality assurance and quality control of the records and data an agency produces. Informational errors can lead to adverse outcomes and liability. Incorrect information in a record can lead to incorrect decision making and improper actions by law enforcement personnel. It can also result in inaccurate data which impacts the ability to produce reliable analysis of crime trends, and resource deployment decisions.

In law enforcement, records management should not be classified as clerical work; it is a specialized discipline requiring legal knowledge, analytical skills, technical proficiency, ethical judgment, and leadership.

Errors, delays, or non-compliance in records operations can result in civil liability, wrongful arrests, inaccurate crime statistics, court sanctions, and reputational damage to agencies.

This guide, and the CLERM certification, reflects the evolving role of records professionals as compliance leaders, quality control experts, and advocates for modern, efficient, and digital records practices.

The guide establishes a defensible, professional standard for certification and practice in law enforcement records management. It aligns training, assessment, leadership, and ethics into a unified national framework that elevates the profession and supports the mission of the Institute for Public Safety Records Management.

Certification Criteria

The CLERM certification emphasizes leadership, planning, policy, strategy, and enterprise-level records management oversight. The certification was developed, and is administered, by the Institute for Public Safety Records Management (IPSRM), founded by PRI. PRI is the leading service provider of public safety information management compliance and standards training for government agencies. Founded in 2008, PRI has trained over 40,000 personnel across the United States, and has developed over thirty courses, some of which are certified by national industry standards and certification organizations including IIMC, ICRM, NAGARA, and ARMA, as well as various state-level organizations.

IPSRM is governed by an Advisory Board comprised of subject matter experts who have peer-reviewed the courses required for CLERM certification. These courses have been uniquely built and curated by IPSRM, based upon PRI curriculum which has been customized and tailored for the CLERM certification.

The CLERM certification requires completion of five on-demand, interactive classes and quizzes which encompass learning the nine domains of knowledge required of records management supervisory and management-level personnel. Each domain includes descriptions of corresponding learning objectives relative to achieving the CLERM certification. These domains are:

DOMAIN 1: Foundations of Records Management Operations

DOMAIN 2: Records Inventory, Retention, and Disposition

DOMAIN 3: Compliance Areas in Law Enforcement Records Management

DOMAIN 4: Sealing and Expunging Records

DOMAIN 5: Quality Control and Case Management

DOMAIN 6: Technology and Digital Records Management

DOMAIN 7: Command, Leadership, and Management of Records Units

DOMAIN 8: Performance Measurement and Continuous Improvement

DOMAIN 9: Professionalism and Communication

Eligibility

Members of IPSRM are eligible for completing the CLERM classes (14 hours) and achieving certification. All members are governed by the following Code of Ethics:

Code of Ethics

Preamble

This Code of Ethics outlines the core values and professional standards that guide the behavior and decision-making of all members of IPSRM. As stewards of sensitive public safety information, members are committed to upholding the highest levels of integrity, accountability, respect for privacy, and compliance with the law.

1 Integrity and Honesty

Members will:

- Maintain the highest standards of honesty and integrity in all professional activities.
- Avoid any conduct that could compromise public trust or the credibility of the organization.
- Report data and findings accurately, without alteration or misrepresentation.

2 Confidentiality and Privacy

Members will:

- Safeguard all records and personal information from unauthorized access, disclosure, or misuse.
- Comply strictly with all applicable privacy laws, including but not limited to CJIS standards and local jurisdictional requirements.
- Only share information with individuals who have legal, authorized access.

3 Transparency and Accountability

Members will:

- Maintain open and transparent operations, except where confidentiality is legally required.
- Be accountable for actions and decisions, and accept responsibility for the outcomes.

4 Compliance with Laws and Regulations

Members will:

- Adhere to all relevant federal, state, and local laws governing records management and public safety data.
- Stay informed about regulatory changes and ensure organizational practices reflect current legal standards.
- Cooperate with lawful investigations, audits, and oversight authorities.

5 Professionalism and Competence

Members will:

- Demonstrate professionalism through respectful conduct, reliability, and continuous improvement.
- Pursue ongoing training and development to remain competent in current technologies, standards, and best practices.
- Refrain from using position or access for personal gain.

6 Impartiality and Fairness

Members will:

- Treat all individuals and record subjects impartially, regardless of race, gender, religion, background, or status.
- Avoid conflicts of interest or the appearance thereof in decision-making and records handling.
- Ensure that all record-keeping reflects fairness and neutrality.

7 Security and Data Integrity

Members will:

- Follow industry-standard data protection measures including access control and secure storage.

- Ensure that all records are accurate, complete, and unaltered except by authorized personnel with proper documentation.
- Respond promptly to data breaches or suspected security incidents.

8 Ethical Use of Technology

Members will:

- Use technology responsibly, ensuring that systems and software support ethical record-keeping practices.
- Regularly evaluate and update digital tools to align with ethical, legal, and operational standards.
- Avoid technologies that enable surveillance or data collection practices that violate individual rights.

9 Respect for Stakeholders

Members will:

- Treat all colleagues, law enforcement partners, and members of the public with respect and courtesy.
- Listen to concerns and complaints, and address them in a timely and fair manner.
- Promote a culture of ethical awareness throughout the organization and among partners.

Amendments and Updates

This Code of Ethics may be amended or updated as necessary, with approval from the IPSRM Advisory Board. All members are expected to familiarize themselves with any changes or updates to this Code.

CLERM LEARNING DOMAINS

CLERM certification courses encompass learning objectives in the nine domains listed below.

DOMAIN 1: Foundations of Records Management Operations

1.1 Records Management Principles

- Legal definition of a record and the records lifecycle
- Active vs. inactive records
- Records series and classifications
- Official (record copy) vs. duplicate records
- Single source of truth concept

1.2 Legal and Regulatory Framework

- State records laws and administrative codes
- Role of state archives / libraries / records agencies
- Local government requirements and approvals
- Documentation of records destruction
- Custodian of Records responsibilities

1.3 Ethical Responsibilities

- Integrity and accuracy of records
- Confidentiality and privacy
- Impartial application of law and policy
- Professional accountability

DOMAIN 2: Records Inventory, Retention, and Disposition

2.1 Records Inventories

- Purpose of records inventories
- Inventory planning and governance
- Division-based inventory approach
- Measuring paper and electronic records
- Inventory documentation requirements

2.2 Retention Schedules

- Purpose and function of retention schedules
- State-provided vs. agency-developed schedules
- Permanent vs. temporary records
- Crime-based retention considerations
- Applying statutes of limitation

2.3 Records Purging and Destruction

- Legal authority to destroy records
- Annual purge programs
- First-pass and second-pass review methodology
- Exclusions: litigation, investigations, holds, audits, evidence, public records requests
- Documentation and certification of destruction

2.4 Post-Purge Analysis

- Evaluating purge outcomes
- Identifying digitization opportunities
- Preventing future backlogs

DOMAIN 3: Compliance Areas in Law Enforcement Records

3.1 Public / Open Records Compliance

- Statutory response timelines
- Redaction principles
- Fee assessment
- Risk management in disclosure

3.2 NIBRS and Crime Data Integrity

- NIBRS purpose and structure
- Data quality standards
- Error identification and correction
- Quality control responsibilities of records units

3.3 CJIS and Information Security

- Access controls and audits
- Data handling requirements
- Security awareness and training

3.4 Validations

- NCIC and state system validation requirements
- Re-contacting victims
- Documentation standards
- Audit readiness

DOMAIN 4: Sealing and Expunging Records

4.1 Purpose and Risk

- Legal intent of sealing and expungement laws
- Civil liability for improper or delayed processing

4.2 Legal Definitions

- Sealed vs. expunged records
- State-specific variations
- Eligibility limitations

4.3 Processing Pathways

- Petition-based court orders
- Automatic / Clean Slate laws

4.4 Processing Methods

- Redaction
- Case locking / restricted access
- Destruction (where legally required)

4.5 Tracking and Certification

- Court Order tracking procedure
- Statutory deadlines
- Notifications and certifications

DOMAIN 5: Quality Control and Case Management

5.1 Report Review and Approval

- Two-level review models
- Authorized corrections vs. rejections
- Documentation of changes

5.2 Case Status and Disposition

- Accurate case lifecycle management
- Coordination with courts, prosecutors, and evidence units
- Impact on retention and reporting

5.3 Risk Prevention

- Preventing misinformation
- Ensuring investigative records integrity

DOMAIN 6: Technology and Digital Records Management

6.1 Digital Records Principles

- Electronic records as official records
- Uniform Electronic Transactions Act (UETA)
- Digital signatures and workflows

6.2 Systems Governance

- Proper use of RMS as the system of record
- Avoiding duplication across systems
- Records request management platforms

6.3 Technology Projects

- Needs assessments
- Procurement and RFP processes
- Implementation and training
- Project closeout and lessons learned

DOMAIN 7: Command, Leadership, & Management of Records Units

7.1 Organizational Structure

- Position-based work allocation
- Records liaisons and coordinators
- Avoiding siloed workflows

7.2 The Four Pillars of Records Operations

1. Business Process
2. Compliance
3. Technology
4. Performance Data

7.3 Leadership Development

- Leading self, others, functions, and the enterprise
- Leadership traits vs. styles
- Professional conduct and accountability

7.4 Policy and Procedure

- Records management policies
- Procedural manuals
- Training requirements
- Continuous policy review

DOMAIN 8: Performance Measurement and Continuous Improvement

8.1 Key Performance Indicators (KPIs)

- Report turnaround time
- Error rates
- Public records response times
- Employee productivity

8.2 Data-Driven Management

- Establishing baselines
- Setting annual and quarterly goals
- Using data to prevent backlogs

8.3 Strategic Planning

- Vision and mission development
- Strategic plans and objectives
- Stakeholder communication

DOMAIN 9: Professionalism and Communication

9.1 Professional Conduct

- Representation of the agency
- Ethical decision-making
- Respectful workplace behavior

9.2 Executive Communication

- Meetings and facilitation
- Written and oral presentations
- Communicating risk and value to leadership