CERTIFIED LAW ENFORCEMENT RECORDS PROFESSIONAL (CLERP)

GUIDE TO CERTIFICATION

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

Certified Law Enforcement Records Professional

Overview and Pricing Information

Public safety 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.

Achieve certification as a Certified Law Enforcement Records Professional (CLERP) by becoming a member of the Institute for Public Safety Records Management (IPSRM).

Membership Includes:

- Ability to achieve CLERP Certification. This requires completion of the six on-demand classes and quizzes included in this membership:
  - » Introduction to Law Enforcement Records Management
  - » A Primer on NIBRS: Doing it Right
  - » Reviewing and Approving Reports in Records
  - » Introduction to Public Records
  - » NCIC: Overview, Risks and Best Practice
  - » Ethics
- Certification certificate mailed to member
- Digital certification badge for use on website and email signatures
- Access to the member forum.
- Access to member-only resources including sample records management policies, guides and tools.
- Access to member-only events including *The Records Room Live* podcast, webinars, and free training sessions.
- Access to post on and view the records Job Board to help with recruiting.

About CLERP Courses

- All courses taken online at your own pace through the IPSRM website (**policerecordsmanagement.com/institute**)
- Courses range from 1-4 hours. Total certification hours: **15**
- Each class has a student worksheet for notes
- Each class has an online 20 question quiz requiring **80%** passing grade

Pricing Per Member

- Initial certification fee first member: **$299**
- 2nd member 25% off **$224.25**
- 3rd member 35% off **$194.35**
- 4th person (or more) 50% off **$149.50**

Annual membership and certification maintenance fee (first year included/no fee): **$99 per member**

CERTIFIED LAW ENFORCEMENT RECORDS PROFESSIONAL (CLERP) GUIDE TO CERTIFICATION

Purpose and Use of this Guide

This guide defines the essential knowledge required of personnel working in or preparing for basic law enforcement records management positions who seek certification as a Certified Law Enforcement Records Professional (CLERP). It serves as the foundational framework for the CLERP 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 core professional law enforcement records management activities for line-level personnel;
- 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 CLERP 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, compliance, 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

The CLERP certification orients records professionals to key elements of records management in public safety including public records, NIBRS data accuracy, quality control of records, NCIC, and ethics. 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 CLERP certification. These courses have been uniquely built and curated by IPSRM, based upon PRI curriculum which has been customized and tailored for the CLERP certification.

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

DOMAIN 1: Foundations of Law Enforcement Records Management

DOMAIN 2: Legal Framework: Retention and Destruction of Records

DOMAIN 3: A Primer on Public Records

DOMAIN 4: Ethics and Professional Responsibility

DOMAIN 5: Report Review, Quality Control, and Case Accuracy

DOMAIN 6: NIBRS Fundamentals and Crime Data Integrity

DOMAIN 7: Case Management and Status/Disposition Control

DOMAIN 8: NCIC, System Integrity, and Information Security

DOMAIN 9: Electronic Records and Digital Workflows

Eligibility

Members of IPSRM are eligible for completing the CLERP classes (15 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 HIPAA, 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.

CLERP LEARNING DOMAINS

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

DOMAIN 1: Foundations of Law Enforcement Records Management

1.1 Records as Government Assets

- Definition of a public/government record
- Records regardless of format, medium, or system
- Official record vs. convenience copies
- Importance of accuracy and completeness

1.2 Records Lifecycle

- Creation and receipt of records
- Processing and maintenance
- Use and dissemination
- Retention and lawful disposition

1.3 Records Categories in Law Enforcement

- Criminal records
- Traffic records
- Administrative records
- Civil records (where applicable)

1.4 Roles and Responsibilities

- Duties of records professionals
- Relationship to sworn personnel and supervisors
- Accountability and chain of custody

DOMAIN 2: Legal Framework: Retention and Destruction of Records

2.1 Records Laws and Authority

- State records management statutes
- Administrative codes and regulations
- Policies and procedures

2.2 Records Retention Schedules

- Purpose and structure of retention schedules
- Record series identification
- Event-based vs. time-based retention

2.3 Destruction and Disposition

- Lawful authority to destroy records
- Prohibited destruction and legal holds
- Documentation of destruction

2.4 Audit and Compliance Readiness

- Maintaining documentation
- Responding to audits and inquiries
- Personal and agency liability considerations

DOMAIN 3: A Primer on Public Records

3.1 Public Records Principles

- Presumption of openness and burden of justifying withholding
- Records vs. information requests
- Statutory response timelines

3.2 Exemptions and Confidentiality

- Common law enforcement exemptions
- Confidential vs. exempt records
- Partial release and redaction principles

3.3 Processing and Release

- Intake and tracking of requests
- Review and redaction processes
- Fee assessment and cost recovery

3.4 Risk Management

- Consequences of improper release
- Consequences of improper withholding
- Documentation of release decisions

DOMAIN 4: Ethics and Professional Responsibility

4.1 Ethics in Public Service

- Ethics vs. morals
- Professional ethics in government
- Public trust and accountability

4.2 Ethical Risks in Records

- Misuse of system access
- Unauthorized disclosure
- Improper destruction or alteration

4.3 Confidentiality and Proper Use

- Need-to-know vs. right-to-know
- Law enforcement databases for official use only
- Handling sensitive and traumatic information

4.4 IPSRM Code of Ethics

- Integrity and honesty
- Confidentiality and privacy
- Professional competence and impartiality

DOMAIN 5: Report Review, Quality Control, and Case Accuracy

5.1 Purpose of Report Review

- Reports as legal documents
- Records unit as quality control gatekeeper
- Draft vs. approved reports

5.2 Error Identification

- Material vs. non-material errors
- Consistency between narrative and data fields
- Missing or conflicting information

5.3 Correction and Rejection Processes

- Authorized corrections
- Report rejection procedures
- Documentation of changes and supplements

5.4 Impact of Errors

- Court and prosecution impacts
- Crime reporting accuracy
- Agency liability and credibility

DOMAIN 6: NIBRS Fundamentals and Crime Data Integrity

6.1 Purpose of NIBRS

- National crime data collection standards
- Importance of accuracy and consistency

6.2 Core NIBRS Concepts

- Offense definitions vs. state statutes
- Group A vs. Group B offenses
- Lesser-included and mutually exclusive offenses

6.3 Incident Structure Rules

- Time and place rules
- Single vs. multiple incidents
- Jurisdictional responsibility

6.4 Records Role in NIBRS Quality

- Detecting errors during review
- Coordinating corrections with officers
- Preventing over- and under-reporting

DOMAIN 7: Case Management and Status/Disposition Control

7.1 Case Lifecycle Management

- Case creation and assignment
- Ongoing updates and supplements

7.2 Case Status

- Open, closed, inactive, and suspended cases
- Proper use of status codes

7.3 Case Disposition

- Cleared by arrest
- Exceptional clearance
- Unfounded or inactive cases

7.4 Impact of Case Errors

- Clearance rate accuracy
- Court and statistical impacts

DOMAIN 8: NCIC, System Integrity, and Information Security

8.1 Purpose of NCIC

- The nexus between records and NCIC
- National information sharing
- Officer and public safety implications

8.2 Data Accuracy and Timeliness

- Entry, modification, cancellation, and validation
- Hit confirmation responsibilities

8.3 Security and Access Control

- Authorized access only
- User credentials and auditing

8.4 Operational Risk

- Consequences of incorrect entries
- Escalation and correction procedures

DOMAIN 9: Electronic Records and Digital Workflows

9.1 Electronic Records as Official Records

- Legal authority for electronic records
- RMS as the system of record

9.2 Scanning and Source Documents

- When scanning is permitted
- Retention of original records

9.3 Digital Workflows

- Electronic forms and signatures
- Secure transmission to partners

9.4 Paper Reduction and Efficiency

- Identifying paper-driven inefficiencies
- Supporting digital transformation at the operational level