COUNCIL POLICY

911 Operations Records Retention

Policy Title	911 Operations Records Retention		
Policy Number	506	Approved Date	2025/12/08
Department	Emergency Management	Last Amended	
Mayor Signature	"J. Clayton" (signed)	Last Reviewed	
		Signature Date	2025-12-11

1. Policy Statement

1.1. The City of Grande Prairie is committed to the responsible records management and security stewardship of all 911 related Operational Records and quality assurance records, including but not limited to Call Audio Recordings, Computer-Aided Dispatch (CAD) logs, incident reports, and System Access Logs. This includes ensuring that records are retained for legislatively mandated periods, are readily accessible for authorized use and are securely disposed of when no longer required.

1.2. In accordance with the *Protection of Privacy Act, SA 2024, c. P-28.5* (POPA), the *Access to Information Act, SA 2024, c A-2.2)* (ATIA), the *Emergency 911 Act, SA 2013, c. E-7.5*, and other applicable laws, all 911 records shall be retained for legislatively mandated periods, accessible for authorized purposes, and securely destroyed when no longer required.

1.3. This policy affirms the City of Grande Prairie's obligation to:

1.3.1. Maintain accurate and reliable records of all 911 activities.

1.3.2. Meet legal, regulatory and operational retention obligations.

1.3.3. Protect Personal Information and operational data from unauthorized access or disclosure.

1.3.4. Classify and protect sensitive Confidential Information and Personal Information

1.3.5. Ensure consistent and Secure Destruction of records post-retention.

1.3.6. Promote accountability, transparency and auditability in 911 service delivery.

1.4. All Employees, contractors and support personnel must adhere to this policy, any related procedures and the Records Retention Schedule.

2. Purpose

2.1. The purpose of this Council policy (policy) is to establish a standardized framework for the creation, management, retention and Secure Destruction of all records created, received or maintained by 911 operations under the authority of the City of Grande Prairie. This ensures compliance with all applicable legislation, supports accountability in emergency response, protects the privacy and legal rights of individuals whose information is recorded, and strengthens operational integrity.

3. Scope

3.1. This policy applies to all 911 operations personnel (including dispatchers, Supervisors and ITS), contractors, and service providers who create, access, manage, or dispose of 911-related records or systems.

4. Definitions

In this policy:

4.1. **"Access to Information Act"** or **"ATIA"** means the Alberta legislation governing the public's right to access records held by public bodies, subject to specific exceptions.

4.2. **"Call Audio Recording"** means a digital recording of incoming or outgoing calls handled by 911 dispatchers, containing real-time caller and dispatcher dialogue.

4.3. **"City"** means the municipal corporation of The City of Grande Prairie, having authority under the *Municipal Government Act, RSA 2000 c. M-26* and other applicable legislation. Where context requires, City also means the area included within the municipal boundaries of the City.

4.4. **"Computer-Aided Dispatch"** or **"CAD"** means a digital system that logs and tracks emergency calls, response actions, and unit deployments.

4.5. **"Confidential Information"** means information, including Personal Information, that could result in harm or operational compromise if disclosed.

4.6. **"Digital Records"** means information related to 911 operations that is created, stored or transmitted electronically. These records are maintained in computer systems or on digital storage media. Examples include:

- **a.** CAD system data and 911 call audio files.
- **b.** Electronic reports or case files.
- **c.** E-mails and electronic messages, including teams messages.
- **d.** Digital photos or video recordings.

4.7. **"Disposition"** means the final action taken with a record (e.g.: Secure Destruction, transfer or archives).

4.8. **"Employee"** means a City employee, including any temporary, casual or permanent employee of the City. For the purpose of this policy, the employee definition also includes a City contractor, or other party who is otherwise required to comply with this policy in accordance with contract terms and applicable law.

4.9. **"ITS"** means Information Technology Services, which provides technical support to 911 Operations.

4.10. **"Legal Hold"** means a directive to preserve all records relevant to a pending or reasonably anticipated legal matter, overriding normal retention timelines.

4.11. **"Operational Records"** means core records documenting emergency response activities (e.g.: calls, dispatch logs, incident summaries).

4.12. **"Personal Information"** means any recorded information about an identifiable individual, including names, contact details, addresses, phone numbers, voice recordings or health information.

4.13. **"Physical Records"** means information related to 911 operations that exist in paper or other tangible form. These records are manually handled and stored in physical files or secure locations. Examples include:

- **a.** Printed call logs or incident reports.
- **b.** Handwritten notes or forms.
- **c.** Hard copy correspondence (letters, faxes, memos).
- **d.** Printed maps or diagrams.

4.14. **"Records Retention Schedule"** means a tool identifying how long different categories of records must be kept and how they are to be securely destroyed.

4.15. **"Secure Destruction"** means irreversible disposal of Physical or Digital Records using certified methods (e.g.: shredding, digital wiping).

4.16. **"Supervisor"** means the Supervisor for the GP911 dispatch operations.

4.17. **"System Access Log"** means a digital record that tracks logins and activities within 911 systems for auditing and cybersecurity purposes.

5. Interpretation

5.1. Where this policy refers to any act, regulation, or City bylaw or policy, it includes the reference to any act, regulation, or City bylaw or policy that may be amended or substituted in its place.

6. General Principles

6.1. Necessity and Proportionality

6.1.1. Only Personal Information that is directly relevant and necessary for the operation of 911 services shall be collected, used or retained.

6.2. Purpose Limitation

6.2.1. Records shall only be used for the purposes for which they were originally collected or for a use consistent with that purpose as defined under POPA.

6.3. Data Minimization

6.3.1. The amount and type of Personal Information retained shall be limited to the minimum necessary to meet operational or legal obligations.

6.4. Security and Safeguards

6.4.1. Records must be protected using appropriate administrative, technical and physical safeguards based on sensitivity.

6.5. Retention and Disposal

6.5.1. Records shall be retained only as long as required by law or operational need and must be securely destroyed when no longer needed.

6.6. Transparency and Access

6.6.1. Access to records must be limited to authorized personnel only. Individuals have a right to request access to their Personal Information, subject to the ATIA.

7. Classification and Security Safeguards

7.1. All records must be protected in accordance with their sensitivity level:

7.1.1. **Public / Internal:** routine or administrative documents (e.g.: schedules, procedures).

7.1.2. **Confidential:** includes incident reports, interagency communications or identifiable caller data.

7.1.3. **Highly Confidential:** involves health emergencies, law enforcement operations, vulnerable persons or active investigations.

7.2. Safeguards must include:

7.2.1. Role-based access permissions.

7.2.2. Encrypted storage for Digital Records.

7.2.3. Locked cabinets for Physical Records.

7.2.4. Regular audits of System Access Logs.

8. Retention and Disposition

8.1. Records must be retained according to the Records Retention Schedule.

8.2. Retention periods being on the date of last activity or record closure.

8.3. Records subject to Legal Hold must not be altered or destroyed until the hold is formally lifted.

8.4. After expiry of the retention period, records must be destroyed using Secure Destruction methods (e.g.: shredding, digital wiping, certified vendor services).

8.5. All Disposition actions must be documented for audit purposes.

9. Roles & Responsibilities

9.1. City Council will review and approve any revisions to this policy.

9.2. City Manager will review and approve any procedures related to this policy.

9.3. 911 Operations Manager oversees Employee compliance, reviews training and enforces the policy.

9.4. Privacy and Access Coordinator ensures that collection and disclosure of Personal Information complies with POPA and manages Legal Holds and breach investigations.

9.5. ITS maintains secure storage, access controls and implements digital Secure Destruction of records.

9.6. City Administration will carry out this policy based on established procedures.

10. Related Information

The following principles guide how Personal Information is managed by the City:

10.1. **Bylaw C-1348** Records Management

10.2. **Council Policy 500** Access to Information and Protection of Privacy

10.3. **Council Policy 502** Safeguarding Privacy

10.4. Information Security and Classification Guidelines

10.5. 911 Operators Manual / Standard Operating Procedures

10.6. Records Classification and Security Safeguards Manual

10.7. Data Breach and Incident Response Policy

11. Legislative Authority

11.1. Municipal Government Act, RSA 2000, c M-26

11.2. Alberta Evidence Act, RSA 2000, c. A-18

11.3. Police Act, RSA 2000, c. P-17

11.4. Emergency 911 Act, SA 2013, c. E-7.5

11.5. Protection of Privacy Act, SA 2024, c. P-28.5

11.6. Access to Information Act, SA 2024, c. A-1.4

12. Review and Revisions

This policy and the accompanying retention schedule will be reviewed every two years, or earlier if:

12.1. Legislative or regulatory changes occur.

12.2. New record types are introduced.

12.3. Risk assessments or audits recommend revisions.

13. Version History

Action	Date	Description
New Policy	2025/12/08	