# DALTON POLICE DEPARTMENT

	Effective Date	Number
	May 1, 1998	GO89-2.23
Subject	•	
<b>Records Management System</b>		
Reference		Revised
CALEA Standards – 11.4.1, 82.1.1, 82.1.4, 82.1.5, 82.1.6, 82.2.3, 82.2.4, 82.3.4, 82.3.5		October <del>27, 2020</del> 25, 2022
Distribution	Re-evaluation Date	No. Pages
All Personnel	October 2022 2024	16

## I. Policy

It is the policy of the Dalton Police Department to operate and maintain various systems designed to manage data, information, and other hardware and computer systems intended to assist employees with achieving the Department's mission.

## II. IT Department Function

The City of Dalton's Information Technology (IT) Department is responsible for managing the Department's computer systems, serving as system security administrator, and serving as system coordinator. The IT Department provides information and support to other components of the Department, researches and designs programs for the Department and its computer systems, serves as computer coordinator, and responds to user requests and problems regarding hardware and software.

#### III. Definitions

- A. *User* A person who utilizes the system on a regular basis or makes periodic requests of the system.
- B. Records Management System (RMS) Refers to the computerized system the Department uses to record, catalog, retrieve, and analyze data collected by the Department and other sources. The RMS is comprised of combinations of hardware components and application software, but includes all other data gathered by peripheral hardware, software, employee input, and other human and electronic resources.

## IV. Administrative Reporting System

The administrative reporting system provides management with information regarding Department activities on a daily, monthly, and annual basis.

A. The shift / section report, a summary of police activity that occurred during the shift, shall be completed at the end of each shift or detail and shall be transmitted via electronic mail and other means, as necessary, to all personnel. The Watch

Commander shall be responsible for this report.

- B. The monthly activity report shall be a summary of Department activity and shall include activity totals for criminal activity, service activity, and arrests. This report shall be completed by the Intelligence Analyst and shall be generated through the use of the RMS. This report shall be transmitted via electronic mail and other means, as necessary, to all Supervisors.
- C. An annual summary of comparative data and statistics relating to the various components of the Department shall be compiled by the Assistant Chief of Police. The Chief of Police may use this summary in determining the success of various programs, setting future Department goals, and determining budgeting needs.
- D. A schedule of all periodic reports, reviews, and other activities mandated by applicable accreditation standards shall be maintained by the Chief of Police or his / her designee. The schedule may be reviewed at Command Staff meetings to ensure that all tasks are being completed.

## V. IT Department Administrative Responsibilities

- A. The IT Department shall serve as the day-to-day manager of all Department hardware, software, data devices, telephony, and computer-related processes. On-going duties include, but are not limited to:
  - 1. Conducting and verifying the RMS backup procedures, including at least weekly verification of data integrity.
  - 2. Monitoring systems components for proper configuration, capacity, and function.
  - 3. Contacting and coordinating outside support resources and arranging necessary maintenance, repairs, or upgrades.
  - 4. Managing and completing computer work orders and other requests for hardware and software assistance.
  - 5. Performing an annual evaluation of all system components and processes and forwarding any recommendations in writing to the Chief of Police.
- B. The Division Commander of the Support Services Division is designated as the liaison to the IT Department.
- C. All personnel are responsible for helping to ensure the smooth day-to-day operation of the RMS by notifying the IT Department of problems and potential problems utilizing computer work orders or, in an emergency, direct communication.

## VI. Case Numbering System

A. A single case numbering system is used by the Whitfield County 911 Center for all case numbers that are assigned to personnel of the Department. Unique case

- numbers are assigned in sequential numerical order by dispatchers through a Computer Aided Dispatch (CAD) system. Case numbers are not omitted or duplicated. If a case number is canceled, a record of the cancelation shall be made in the CAD system.
- B. Case numbers shall have eight (8) digits. The first two (2) digits represent the year, followed by a dash. The remaining numbers are the generated case number. For example, the first case number assigned in 2022 was 22-000001. The next case number was 22-000002, etc.

## VII. Status of Reports

- A. After a report within the RMS has been reviewed and approved by a Supervisor, it shall be submitted to the Records Section no later than the next business day.
- B. The Records Section shall use a CAD Case Report Summary printout to compare the case number against the Daily Work Allocation Report to ensure that the original report has been received by the Records Section.
- C. During the approval process, a Supervisor may assign a case for further investigation. The name of the Officer / Investigator assigned for follow-up shall be entered into RMS. Supervisors shall enter a due date into the RMS for a status update within ten (10) days of the assigned date. The Officer / Investigator shall be responsible for reviewing the case and submitting a status update before the due date. Supervisors shall be responsible for ensuring assigned cases are updated according to the prescribed schedule and all follow-up reports are submitted in a timely manner.

# VIII. <u>Data Entry</u>

#### A. Incident Reports

- Law incident reports shall be accurately entered into the Records Management System (RMS). Reports shall be completed in a timely manner, either during or shortly after the shift on which the incident was reported. Supplemental reports shall be entered by the appropriate Officer or Investigator during follow-up.
- 2. All documents, images, or electronic files shall be added to the RMS and linked to the correct law incident report(s), or, in some cases, entered into the Property and Evidence Section.
- 3. Original and supplemental reports shall be reviewed by the appropriate Supervisor as soon as possible after submission. Supervisors shall return the report to the originating Officer for correction if there are errors.
- 4. Upon final approval, the Supervisor shall electronically forward all reports to the Records Section.

- 5. The Records Section shall audit all reports for accuracy, completeness, and NIBRS compatibility. If discrepancies are noted that need correction by the Officer, the Records Section shall notify the Officer.
- 6. Upon final completion, the Records Section shall move each report to the partitioned area of the RMS to maintain long-term integrity and guard against accidental changes. All partitioned reports shall be visible to Department members based on normal user permissions, but in a read-only capacity. Reports may be moved out of the partitioned area for further processing at the discretion of a Division Commander.
- 7. At the discretion of the Chief of Police, certain reports may be temporarily locked from general view during an active investigation.

#### B. Traffic Collision Reports

- Traffic collision reports shall be completed accurately by the investigating Officer using the Georgia Electronic Accident Reporting System (GEARS). Reports shall be completed in a timely manner, either during or shortly after the shift on which the collision was reported.
- 2. Supervisors shall be responsible for reviewing each traffic collision report for accuracy and completeness. Supervisors shall review and approve or disapprove each report, rejecting reports with errors back to the Officer for correction. The reports are maintained within the GEARS database.

# C. Field Interview Reports

- 1. Field Interview Reports (FIR) shall be entered accurately into the RMS by the originating Officer / Investigator during his / her tour of duty.
- 2. Supervisors shall be responsible for reviewing each FIR for accuracy and completeness. Upon approval, the FIR shall be forwarded electronically to the Records Section.
- 3. The Records Section shall be responsible for auditing all FIRs for accuracy, notifying the Officer / Investigator of any errors.

### D. Traffic Citations

- 1. Officers are responsible for accurately entering traffic citation information into the appropriate citation software, which forwards the citation automatically to the RMS via the designated manner.
- 2. With Supervisor approval, Officers may issue paper citations, which shall be forwarded to the Records Section. The Records Section is responsible for manually entering paper citation data into the RMS.
- 3. The Records Section shall review each citation and written warning submitted to the RMS and verify that the offense location is properly geo-

coded. The Records Section shall coordinate with the IT Department if assistance is needed in verifying the location or other data.

# E. Data Entry Standards

- 1. Data entered into all Department paper and electronic records must comply with the Data Entry Standards outlined in Appendix A.
- 2. Every Supervisor and Manager in the Department is responsible for ensuring that data is accurate, as complete as possible, and in conformance with the Data Entry Standards.

## F. Evidence and Property Data Entry

A Property and Evidence Technician (PET) shall be responsible for the entry of all evidence and property records within twenty-four (24) hours after having received them.

### G. Training Data Entry

The Training Coordinator Support Services Division shall be responsible for the entry of all academy / technical training, formal education, and various qualifications and certifications, after having received a record of said training or qualification, into the recipient's training file.

# H. Personnel Data Entry

The Chief of Police's Administrative Assistant is responsible for accurate entry into the RMS of all personnel data, including but not limited to:

- 1. Commendations / Awards
- 2. Promotions
- 3. Disciplinary action
- 4. Assignments and transfers
- 5. Payroll changes
- 6. Personal information

## I. Issued Equipment Entry

PETs are responsible for accurate entry into the RMS of all Department and individual-issued property and equipment.

#### J. Vehicle Fleet Data

PETs are responsible for the accurate entry into the RMS of all vehicle fleet maintenance, repair, and fuel usage data.

## IX. Accountability for Traffic Citations

Traffic citations shall be accounted for from the point of issuance to the individual Officer through final adjudication by the court.

#### A. Issuance of Manual Citation Books

After the issuance of a manual citation book, the Officer shall initiate a record of the citation book to include citation numbers, Officer's name, and the date issued. After completion, the record shall be turned into a Supervisor for approval.

#### B. Issuance of Electronic Citations

The IT Department shall be responsible for assigning ticket ranges for the electronic citation system. Electronic citation numbers are issued to Officers at the point of submission and then uploaded into the RMS.

### C. Citation Audits

- A documented citation audit shall be conducted annually by the Patrol Division Commander or his / her designee. The audit shall consist of a sufficient representative sample of electronic and manual citations to ensure citations are accounted for.
- 2. If deemed necessary, the Chief of Police or Patrol Division Commander may direct any additional audits to be conducted on electronic or manual citations.
- 3. Lost or stolen citations shall be reported to the Patrol Division Commander via written memorandum.
- 4. The Patrol Division Commander shall make every effort to locate the citation(s) and, if not found, shall prepare a memorandum to the Chief of Police.
- 5. The memorandum shall list the citation number(s), results and explanation of the investigation of the lost or stolen citation(s), and actions taken.

## D. Security of citations

- 1. All un-issued electronic citations shall be password protected and maintained by the IT Department until issued.
- 2. All un-issued manual citations shall be maintained in a secure area, accessible to Supervisors, until time of issuance.

# X. Privacy and Security of Central Records

A. Designated Department records in hard copy shall be maintained in the Records Section with accessibility for operations personnel, 24 hours a day.

- B. Electronic Department records are accessible to employees at all times, via the Department's RMS, with security access and limitations inherent within each user's log-in and password / passphrase. Passwords and passphrases shall be in compliance comply with the standards as determined by the Support Services Division Commander set by the IT Department.
- C. Physical access to the Records Section is controlled through an electronic keypad and is limited to employees and contractors with a legitimate need for access.

## XI. Release of Department Records

- A. Persons requesting information and / or records shall make the request by telephone, by mail (electronically or digitally), or in person at the Records Section window located on the first floor of the Police Services Center.
- B. Records shall only be released in accordance with Georgia's Open Records Act. If a question arises concerning the release of records, the Support Services Division Commander shall make the determination as to the release and is authorized to seek guidance from the City Attorney regarding compliance with the Georgia Open Records Act.

# XII. <u>Distribution of Reports / Records</u>

- A. Incident and supplemental reports are completed in RMS and are stored electronically. Traffic collision reports are completed and stored within the GEARS system.
- B. Copies of originals or computer-printed copies shall be used when records are approved for release.
- C. The Department also participates in the National Incident-Based Reporting System (NIBRS) program. The records gathered are submitted electronically to the Federal Bureau of Investigation's NIBRS program.
- D. Anytime an employee completes a report of a juvenile or adult that needs followup action by the Department of Family and Children Services or Adult Protective Services, the employee shall fax or email transmit the report to the appropriate agency utilizing an Department fax machine or device approved transmittal method.

#### XIII. Criminal History Records

The computerized criminal history files for the State of Georgia are maintained by the Georgia Crime Information Center (GCIC). At the Department, criminal history records are generated within the Records Section, the Patrol Division, and the Criminal Investigations Division. All areas have controlled access, and each computer with access to GCIC must be accessed via a username and password / passphrase. It is the responsibility of all personnel accessing GCIC criminal history records to ensure that the records are disseminated properly. The following reflects the various situations in which criminal histories may be obtained:

- A. Officers may receive criminal histories for investigative purposes.
- B. With a signed consent form, criminal histories are generated for:
  - 1. All persons who desire to participate in the Ride-Along Program or the Citizen's Police Academy.
  - 2. Persons who wish to have a copy of their own criminal history.
- C. With a signed Criminal History Consent form, individuals can receive limited criminal histories on other persons.

# XIV. Security of the Central Records Computer System

To ensure the integrity of the Department's RMS and all associated electronic data stored on-site, the Department, in coordination with the IT Department, has developed on-going security processes.

- A. Storage / System Backup
  - The Department's computer servers are securely stored within the a designated server room located in the Records Section of the Police Services Center. Limited authorized access is controlled through a keypad entry to the room.
  - 2. The Department's computer servers are backed up by secondary servers that are securely maintained at other City Hall facilities.
  - 3. The IT Department shall ensure a backup of all RMS data takes place on a regular daily basis or more often, as necessary. The backup shall be maintained and secured on a cloud-based storage system.
  - 4. On a weekly basis, the IT Department shall verify that the backup procedures have been successful by analyzing the data contained within the backup.
- B. System Access Security

The Records Management System has controlled access via an employee-specific user name and password / passphrase. Passwords / passphrases shall not be shared with anyone other than members of the IT Department. The level of access an employee has within the RMS coincides with the individual's position in the Department.

#### C. Password Audits

At least annually, the Support Services Division Commander or his / her designee shall conduct an audit of all usernames and passwords. This audit serves to maintain the integrity of the system and the security of the records contained in the system.

## XV. Off-Site Electronic Data Storage

In instances where electronic data is stored off-site using an outside service provider (i.e. PowerDMS, Guardian Tracking), the Department shall establish a written agreement with the service provider to address the following:

- A. Data ownership
- B. Data sharing, access, and security
- C. Loss of data, irregularities, and recovery
- D. Data retention and redundancy
- E. Required reports, if any
- F. Special logistical requirements and financial arrangements

## XVI. <u>Disaster Recovery</u>

- A. In the event of a total or partial failure of data, hardware, or systems, the IT Department shall take immediate action to restore systems, data, and all functions. After conferring with the Chief of Police or his / her designee, the IT Department is authorized to contact outside resources, if needed.
- B. The IT Department shall be responsible for providing a written report of all hardware, software, and system process failures to the Chief of Police. This report should include, at a minimum:
  - 1. Diagnosis of the problem(s) and cause(s)
  - 2. The area(s) and / or function(s) affected
  - 3. Steps taken to correct the problem and resume operations
  - 4. Recommendations on how to avoid the problem or failure from recurring
- C. The IT Department shall be responsible for developing and maintaining a written Disaster Recovery Plan that outlines the following:
  - 1. Detailed description of the Department computer system backup procedures
  - 2. Detailed description of any offsite data storage procedures, including the physical location and method and frequency of data transfer
  - 3. Schematic mapping of all Department network operations, including all connections with Department mobile units and locations outside the Police Services Center (City Hall, other departments, etc.).

# XVII. Internal Records Maintained Outside of the Records Section

Most reports generated by the Department are maintained in the Records Section. Some records, usually those of an administrative or confidential nature or containing such information that renders them more appropriately stored in a specific unit or section, are maintained by various operational components and outside of the Records Section. These records include, but are not limited to, the following:

- A. Office of the Chief of Police Personnel files, personal correspondence files, grievance files, disciplinary records, and critical incident review files.
- B. Criminal Investigations Division Investigative case files and Confidential Informant files.
- C. Support Services Division Professional Standards files, use of force reports supervisory reviews of responses to resistance and / or aggression, employment testing materials, and training records.
- D. Patrol Division Selective traffic enforcement records, active extra patrols, radar / laser records, completed ride-along forms, and completed off-duty / extra-duty applications.

# XVIII. Media Protection

- A. All employees are responsible for ensuring that access to digital and physical media in all forms is restricted to authorized individuals.
- B. All digital and physical media shall be securely stored within physically secure locations or controlled areas.
- C. All employees shall protect and control digital and physical media while transporting or possessing it outside of the controlled access areas of the Police Services Center.
- D. Digital and physical media containing Criminal Justice Information (CJI) shall not be left unsecured and / or visible in vehicles, offices, workspaces, or common areas within the Police Services Center where unauthorized individuals may come in contact with it.

## XIX. Security Incident Reporting / Handling

- A. The City of Dalton's Director of Information Technology is designated as the Department's Local Agency Security Officer and shall be responsible for the following:
  - 1. Identifying who is using the Department's approved hardware, software, and firmware and ensuring no unauthorized individuals or processes have access to the same.
  - 2. Identifying and documenting how the equipment is connected to the State of Georgia's system.

- 3. Ensuring that personnel security screening procedures are being followed, as required by GCIC.
- 4. Ensuring the approved and appropriate security measures are in place and working as expected.
- 5. Supporting policy compliance and ensuring the Department and GCIC are promptly informed of security incidents.
- B. Any mishandling, loss, or inadvertent or inappropriate disclosure of CJI / CHRI shall be immediately reported to the IT Department, Chief of Police, and GCIC.
- C. The loss or compromise of any Department-owned mobile device (smart phone, tablet, etc.) shall be immediately reported to the IT Department and the Chief of Police.
- D. In the case of a security incident, the IT Department shall be responsible for the incident handling, to include preparation, detection and analysis, containment, eradication, and recovery.
- E. All employees with access, including physical and logical access, to GCIC materials, records, and information shall follow the policies, rules, and procedures set forth by GCIC, NCIC, the FBI CJIS Security Policy, and the laws of the State of Georgia.
- F. All employees shall complete Security Awareness training and recertification, as required by GCIC.

# XX. Disposal of Information

- A. Media, both physical and digital, shall be disposed of properly by all employees, contractors, or other personnel with access, to include physical and logistical access to GCIC / NCIC data, sensitive and classified data, and media. This applies to all equipment that processes, stores, and / or transmits CJI, as well as sensitive and classified data.
  - 1. Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:
    - a. Shredding using Department shredders
    - b. Placed in a locked shredding bin for future destruction
  - 2. Electronic media (hard drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the following methods:
    - a. Overwriting (at least 3 times)
    - b. Degaussing

$\sim$	Destru	ICTION
U.	Desilu	IULIUII

B. The IT Department shall be responsible for sanitizing Department computers, systems, and equipment that have been used to process, store, or transmit CJI and / or sensitive and classified data to ensure all stored information has been cleared upon being placed out of service.

This policy supersedes any policies previously issued.

BY ORDER OF

**CHIEF OF POLICE** 

# **APPENDIX A**

Dalton Police Department
Data Entry Standards

All Dalton Police Department personnel shall use the standards and procedures set forth in this document for data entry to enhance accuracy and minimize the duplication of records and data in the system.

All entries made into the system will be made in Upper Case format.

# **Name Entry Standard**

All names shall be entered with as much information as possible (e.g. Last, First, Middle, and Name Suffix). Full Legal Name, if known, shall be used at all times. Abbreviated versions or nicknames shall be listed as an alias to the real name. If parts of the name or other fields are unknown, leave the field blank. Do not enter UNK or NMN in any name field. Middle Initials are permitted, but do not use punctuation. No punctuation is to be used in the name fields except for hyphens and only under special circumstances.

Example:	Last	First	Middle
Correct	SMITH	RONALD	THOMAS
Correct	SMITH	RONALD	Т
Incorrect	SMITH	RON	
Incorrect	SMITH	RONALD	T.

#### Name suffixes

Name suffixes shall not be entered in the last name field. This information will be entered in the suffix name field which is located directly after the middle name field.

#### **Titles**

Titles such as Doctor, Professor, Officer, Deputy, etc. shall not be entered in a name field. The suffix field may be used for titles. Abbreviations for titles are acceptable without the use of punctuation. Examples: MD, PHD, OFF, DEP

If the individual has both a professional title and suffix, the suffix shall be placed in the suffix field and the professional title in the comments field.

#### **Multiple Surnames**

If the legal name is hyphenated, enter the hyphenated name into the data field. The hyphen shall be placed between the two last names. Variations of the name can be added as aliases.

#### Example:

Correct Entry:

Real Name Screen	RODRIGUEZ-VASQUEZ	JOSE	ANGEL
1 <sup>ST</sup> Alias	RODRIGUEZ	JOSE	<b>ANGEL</b>
2 <sup>ND</sup> Alias	VASQUEZ	JOSE	ANGEL

Incorrect Entry	RODRIGUEZVASQUEZ	JOSE	ANGEL
Incorrect Entry	RODRIGUEZ GONZALES	JOSE	ANGEL

Correct Entry:

Real Name Screen	SIMPSON-FIELDS	SHARON	Α
1 <sup>ST</sup> Alias	SIMPSON	SHARON	Α
2 <sup>ND</sup> Alias	FIELDS	SHARON	Α

Incorrect Entry SIMPSONFIELDS SHARON A Incorrect Entry SIMPSON FIELDS SHARON A

#### Names with Apostrophes

Names with apostrophes shall be entered with no apostrophe and no space between the letters. The name shall be entered as a single word.

(OBRIEN and ONEIL should be used instead of O'BRIEN and O'NEIL.)

### **Compound Names**

Compound names shall be entered without spaces. For example, DE LA ROSA shall be entered as DELAROSA, ST. MARIE shall be entered as STMARIE, and VAN HOOSER as VANHOOSER. No punctuation is permitted with compound names.

# **Alias Entry Standard**

Correct Entry:

A separate alias name record shall be created for any name other that the person's legal name. The alias entry shall only contain data in the name field, DOB field, and the SSN field.

An alias should only be entered when the entry person can absolutely state that the name in question refers to the same individual.

# **Business Name Entry Standard**

Enter the name of a business in the last name field only. The word "The" shall be eliminated at the start of the business name for entry into the system. Omit corporate designations, such as INC, CO, and punctuation. Hyphens and ampersands (&) shall be used if they are part of the official name of the business.

#### Example:

control Entry.		
Last: HOUSE OF PAIN	First:	Mid:
Incorrect Entry:		
Last: THE HOUSE OF PAIN	First:	Mid:
Incorrect Entry:		
Last: HOUSE OF	First: PAIN	Mid:

The ampersand (&) shall not be used to replace the "and" in business names, but may be used if the ampersand is a valid part of a business name. If used, the ampersand (&) shall have a space on either side of the ampersand character.

#### Example:

Correct Entry:

Last: BB & T First: Mid:

Incorrect Entry:

Last: BB&T First: Mid:

Business names that are numbers shall be entered as numbers. For example, HIGHWAY 5 CONSTRUCTION, 7-11, ABC 123, are all acceptable methods of entry.

Doctors, Dentists, and Attorney's (the business, not the individual will be entered completely in the last name field. These names should not have any character inserted into the data field.

MARK H LEOPOLD DDS GARY R DONATH MD

# **Address Entry Standard**

Whenever possible, obtain a street address for all names that are entered into the system. A mailing address is the next best option. If both addresses are to be entered, the street address shall be entered into the address field and mailing address shall be added to the comments field. If the mailing address is a post office box, the designated abbreviation is PO BOX 123.

Standards for address entry into the system are based on the U.S. Postal Services Standardized Addressing Guidelines.

#### **Address Parts**

Address shall be in this order: House Number, direction, street name, and street type.

Examples: 1505 W WALNUT AVE

2759 N CEDAR ST

APT, ROOM, SUITE, BUILDING shall not be entered into the address. Simply replace the designation with a semicolon (;) and include the numerical value.

A semi-colon (;) shall be added after the street type for additional identifiers to the address, such as building number, apartment number, etc.

Examples: 1505 W WALNUT AVE; 123

2759 N CEDAR ST; B

#### **Street Names**

All street names will be listed with complete names. No abbreviations shall be used. WAL is not an acceptable for WALNUT AVE.

All numbered streets shall use the numeric symbol. FIRST ST is not acceptable for  $1^{ST}$  ST. FIFTH AVE is not acceptable for  $5^{TH}$  AVE.

# **Fractional Addresses**

Enter all fractional addresses as a fraction. (1/2, 2/3)

#### Intersections

Use a slash (/) to indicate an intersection such as HWY 52/AIRPORT RD

## **City Names**

No abbreviations should be used for city names. DAL is not acceptable for DALTON.

#### **Street Extensions**

The following abbreviations are to be used:

ALY	Avenue	AVE
BLVD	Circle	CIR
CT	Crossing	XING
DR	Highway	HWY
HTS	Lane	LN
LP	Mountain	MTN
PKY	Place	PL
PO BOX	Point	PT
RDG	Road	RD
SR	Street	ST
TER	Way	WY
N	Northeast	NE
E	Northwest	NW
S	Southeast	SE
W	Southwest	SW
	BLVD CT DR HTS LP PKY PO BOX RDG SR TER N E S	BLVD Circle CT Crossing DR Highway HTS Lane LP Mountain PKY Place PO BOX Point RDG Road SR Street TER Way  N Northeast E Northwest S Southeast