


**LANCASTER POLICE DEPARTMENT
GENERAL ORDERS MANUAL**

Effective Date August 26, 2015		Amended Date September 4, 2015 December 12, 2017		Directive 5.01.1	
Subject Records Retention, Privacy and Security					
Reference			Approved  Chief of Police		
Distribution All Personnel City Manager City Attorney		TPCA Best Practices Recognition <i>Program Reference</i> 5.01; 5.02; 10.02		Review Date December 12, 2017	
				Pages 5	

This Operations Directive is for internal use only and does not enhance an officer's civil or criminal liability in any way. It should not be construed as a creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this Operations Directive, if proven, may only form the basis for a complaint by this Department, and only in a non-judicial administrative setting.

SECTION 1 PURPOSE

The purpose of this policy is to establish direction, procedures, and requirements to ensure the appropriate security and privacy of records. The policy will also assign specific responsibilities for the provision of data and security and for the security of the various infrastructure environments.

SECTION 2 POLICY

It is the policy of the department to prohibit unauthorized access, disclosure, use, duplication, modification, diversion, destruction, storage, loss, misuse, or theft of law (hard copy or electronic) records, information. This policy applies to all personnel who have access to computer systems, networking systems, physical records (including electronic mail), peripheral equipment, workstations, personal computers (desktop and portables), within the Lancaster Police Department. Network and computer resources include data, printouts, and telecommunications that permit access to records.

SECTION 3 DEFINITIONS

A. **Authorized personnel:** For the purpose of this order, authorized personnel refers to the following positions:

1. Chief of Police;
2. Support Division Assistant Chief of Police;
3. Recognition Commander;
4. Records Supervisor;
5. Records Clerk;
6. Criminal Investigation Division Technician; and
7. Investigator assigned to sex offender registration

LANCASTER POLICE DEPARTMENT
GENERAL ORDERS MANUAL

<i>Effective Date</i> August 26, 2015	<i>Amended Date</i> September 4, 2015 December 12, 2017	<i>Directive</i> 5.01.1
<i>Subject</i> Records Retention, Privacy and Security		

- B. **Records:** Any complete document kept and/or maintained by the Lancaster Police Department, including but not limited to:
1. offense reports, arrest reports;
 2. juvenile records;
 3. archive records;
 4. sex offender records;
 5. accident reports;
 6. Uniform Crime Reports (UCR);
 7. Incident Based Reporting (IBR) reports; and
 8. all other miscellaneous documents that may accompany these records
- C. **Retention Schedule:** A schedule for managing records governed by the Texas State Library and Archives Commission (TSLAC) which has been adopted by the City Council of the City of Lancaster.
- D. **Custodian of Records:** Refers to any person designated to be in charge of the care and custody of the records maintained by the Lancaster Police Department Records Division.

SECTION 4 PROCEDURES

A. USERS

1. Users are expected to follow all policies and procedures related to records security and privacy of records data in both physical and electronic format. Department personnel will comply with all policies and procedures pertaining to the printing, copying and faxing of records. This includes transmission, viewing and distributing records.
2. Department personnel are expected to know and comply with all existing security and privacy policies. Only authorized department personnel will be given access to the communication infrastructure as relates to records in a capacity limited to meet the ability to perform their duties appropriately and with a need to know level of access only.
3. All department personnel who have been determined to no longer need access to the communication infrastructure or specific areas of the network and applications will be removed from access lists, including terminated employees, employees on extended leave, retired or transferred employees with new duties and responsibilities.

B. SUPERVISORS, MANAGERS, AND DIVISION COMMANDERS

1. Supervisors, managers and Division Commanders are responsible for ensuring that records data privacy and information security measures are being followed for their areas. They are

**LANCASTER POLICE DEPARTMENT
GENERAL ORDERS MANUAL**

Effective Date August 26, 2015	Amended Date September 4, 2015 December 12, 2017	Directive 5.01.1
Subject Records Retention, Privacy and Security		

responsible for ensuring the records security and privacy of all department/agency data stored as either physical paper records or electronic records on departmental computer servers. They will work with the appropriate network and information security administration to ensure records security and they must maintain a current working knowledge of the department's policies pertaining to records security and privacy and identify necessary process improvements and/or changes when new policies are approved.

2. The Records Manager will oversee the lawful management of information, the associated training and the day-to-day implementation of the records security and privacy policies for all Records Division personnel. The Records Manager will receive specialized training related to the release of information, privacy and security of records, and applicable laws. The Records Manager will handle open records requests. Records personnel will handle open records requests in the absence of the Records Manager.

C. PUBLIC INFORMATION OFFICER

1. The designated Public Information Officer (PIO) or an on-duty supervisor in the absence of the PIO is responsible for the department's release of information in compliance with Chapter 552 "Public Information Act," Texas Government Code.

D. SECURITY OF RECORDS

1. The workspaces occupied and maintained by the Records Division are located in a secured portion of the Public Safety Building.
2. Access to the workspaces within the Public Safety Building that are associated with the Records Division are restricted to authorized personnel only. Entry by unauthorized personnel is prohibited.
3. The workspaces will be secured and locked when unmanned by authorized personnel.
4. Arrest and juvenile records are kept in a separately locked closet that is located in the secured records section of the building, in accordance with applicable requirements. (TPCA 5.01, 10.02f)
 - a. The Records Supervisor is issued the primary key for the locked closet containing arrest and juvenile records.
 - b. The position(s) of Records Clerk is allowed access to the secure closet during normal business hours for the Records Division.
5. Sex offender records are kept in locking file cabinet(s) which are secured within the Criminal Investigation Division.
 - a. The investigator assigned to sex offender registration is issued the primary key for the locked file cabinet(s) containing sex offender records.

**LANCASTER POLICE DEPARTMENT
GENERAL ORDERS MANUAL**

Effective Date August 26, 2015	Amended Date September 4, 2015 December 12, 2017	Directive 5.01.1
Subject Records Retention, Privacy and Security		

- b. In the absence of the assigned investigator, the Criminal Investigation Division Supervisor shall take possession of the key and grant access to the investigator conducting sex offender registration for that specific time.
- 6. The Criminal Investigation Division is responsible for compiling, maintaining, storing and disseminating all gang-related intelligence.
- 7. Police records maintained on the computerized Records Management System (Sungard/OSSI) are password protected and not viewable by the public or unauthorized personnel.
 - a. The Chief of Police is responsible for ensuring that the proper rights and securities including usernames and passwords are maintained for all aspects of the Records Management System.
 - b. The task of creating password requirements and parameters shall be performed by the Information Technology Department with the City of Lancaster.
 - c. Records personnel shall ensure that unauthorized personnel cannot see the content on his/her monitor and that all computer monitor screens are "locked" when unattended.

E. VERBAL SECURITY BREACHES

- 1. All Lancaster Police Department personnel who have access to records shall only communicate sensitive information to appropriate personnel. When an employee is in doubt regarding the lawfulness or appropriateness of the information release, then they should not release the information. The employee shall immediately contact the department's Public Information Officer or a supervisor who shall determine if the information is to be released.

F. RECORDS RETENTION (TPCA 5.02)

- 1. The City of Lancaster has standard instructions for records retention, inventory and storage. These instructions include, but are not limited to: (TPCA 5.02)
 - a. Instructions for Preparation of Records Inventory and Storage;
 - b. Retention Schedule for Common Government Records; and
 - c. Retention Schedule for Police Records.
- 2. All records within the Lancaster Police Department may be managed by different divisions, but must follow the retention periods as set forth in the Retention Scheduled.
 - a. Section 441.158, Texas Government Code, provides that the Texas State Library and Archives Commission (TSLAC) shall issue records retention schedules for each type of local government, including a schedule for records common to all types of local government. The law provides further that each schedule must state the retention period described by federal or state law, rule of court, or regulation for a record for which a period is prescribed; and prescribe retention periods for all other records, which periods have the

LANCASTER POLICE DEPARTMENT
GENERAL ORDERS MANUAL

<i>Effective Date</i> August 26, 2015	<i>Amended Date</i> September 4, 2015 December 12, 2017	<i>Directive</i> 5.01.1
<i>Subject</i> Records Retention, Privacy and Security		

same effect as if prescribed by law after the records retention schedule is adopted as a rule of the commission.

- b. The complete detailed information from TSLAC regarding retention of documents may be found on their website: <http://www.tsl.state.tx.us/slrn/recordspubs/ps.html>

G. JUVENILE RECORDS (TPCA 10.02f)

1. All juvenile criminal records are secured in locked file cabinets, completely separate from adult records and other files. (TPCA 5.01)
2. All juvenile records that are maintained by the Lancaster Police Department will be managed based on the juvenile record retention schedule and information from TSLAC. (TPCA 5.02)

H. PROTECTED FILES

1. Records that are expunged or sealed are exempt from the retention schedule.
 - a. **Section 2-1(b):** Arrest and other law enforcement records relating to an individual are subject to expunction under Articles 55.01 to 55.05, Texas Code of Criminal Procedure. An expunction overrides any retention period established in this schedule. The destruction of expunged records is exempt from a destruction request to the Texas State Library.
 - b. **Expunction:** In accordance with a court-ordered expunction, any records pertaining to the court order will be destroyed according to the court order, both in hard-copy form as well as computerized records. A letter of compliance will be sent to the District Clerk's Office advising of compliance with the expunction orders.
 - c. **Order Sealing Juvenile Record:** Any order(s) to seal one or more juvenile records will be treated in the same manner as an expunction. The records requested will be destroyed, both in hard-copy form as well as computerized records. A letter of compliance will be sent to the Dallas County Juvenile Probation Office advising that the order has been complied with.
 - d. **Fulfillment:** All orders of expunction, restricted access, sealed juvenile records, and non-disclosure will be completed by the Custodian of Records.

I. SCOPE OF RESPONSIBILITY

1. All members of the department shall know and comply with all aspects of this directive.
2. All Division Commanders and supervisory personnel are responsible for ensuring compliance with the provisions and intent of this directive.