



# Alexandria Police Department

## Directive 6.1



# SECURITY OF POLICE FACILITIES

Effective Date: 02-03-2016

Cancels: 08-21-2012; Rescinds Directive 12.6- Foreign Visitors to the Department (01-10-2009)

Updated Date: 08-21-2019

Section(s):

SME Review Date:

Updated Date:

Section(s):

2022

Updated Date:

Section(s):

## CONTENTS

6.1.01	POLICY/PURPOSE
6.1.02	AUTHORITY/BACKGROUND
6.1.03	DEFINITIONS
6.1.04	RESPONSIBILITIES
6.1.05	KEYS AND ELECTRONIC ACCESS CARDS
6.1.06	EMPLOYEE & VISITOR IDENTIFICATION
6.1.07	VISITORS TO POLICE FACILITIES
6.1.08	FOREIGN VISITORS
6.1.09	SPECIAL VISITORS AND EVENTS
6.1.10	OTHER POLICE FACILITIES
6.1.11	EMERGENCIES
Appendix A	Authorized Access Categories

### 6.1.01 POLICY/PURPOSE

It is the policy of this Department to secure all police facilities for the safety and comfort of employees and visitors and for the security of confidential information and materials. The purpose of this directive is to establish standards and procedures for maintaining good security at 3600 Wheeler Avenue and all other police work sites.

### 6.1.02 AUTHORITY/BACKGROUND

AR 7-21: PROHIBITION OF CONDUCT AND BEHAVIOR IN CITY FACILITIES.  
As upheld by the Virginia Supreme Court, the City Manager has legal authority to prohibit the possession or use, or any threat to use, a weapon or firearm at a city

work site. The *Alexandria Police Department's* Facilities and Security Management *Section* oversees the administration of the *electronic security* systems.

Units operating at a confidential location(s) will administer their own security plans and systems.

### 6.1.03 DEFINITIONS

#### **Access Report Request Form:**

Official form completed by a Commander when requesting or authorizing electronic card data or video of gaining access to doors, hallways, gates or other areas for matters under review or investigation.

#### **Department Issued Credentials:**

Identification or pass issued by the Police Department to sworn employees, authorized civilian employees, and others (Retirees, Fire Marshal, CA's Office, etc.) as approved by the Chief of Police.

#### **Electronic Access/Photo Identification Card:**

Photo identification card programmed to give access to selected electronically controlled doors at Police Department facilities and work sites issued by the Facilities and Security Management *Section* to all Police employees, Department of Emergency Communications (DEC) employees, and volunteers.

#### **Identification/Pass:**

Identification or pass issued by the Facilities and Security Management *Section* to contractors or visitors. This issued identification may or may not grant access to selected electronically controlled doors.

#### **Police Facility:**

Any property, building, or location under the control of the Office of the Chief of Police.

### 6.1.04 RESPONSIBILITIES

#### **A. Employees are responsible to:**

1. Keep secure in their immediate possession their electronic access/photo identification card, door keys, and Department issued credentials, if applicable.

2. Display employee identification when in Police facilities and not in uniform unless displaying it would compromise safety; i.e., undercover assignments.
3. Return all issued keys to Facilities and Security Management *Section* when transferred to a different unit.
4. Return all electronic access/photo identification cards to the *Facilities and Security Management Section* when retiring or separating from the Department.
5. Return keys to the Security Manager upon completion of an assignment or upon separation from the Department.
6. Immediately report the malfunction of any secure door or *external gate* to the Facilities Security *Management Section*. After business hours, notification shall be made to the Watch Commander. The Watch Commander shall notify the *Security contractor and the Facilities and Security Management Section*.
7. Challenge anyone in a secure area that does not display identification or a proper pass and escort those persons to the Atrium Security Post to obtain a pass.
8. Keep confidential information and materials out of view of visitors or unauthorized persons.
9. Exercise sound judgment in the monitoring and escorting of visitors. *All contractors will be signed in and escorted at all time while they are in the facility.*
10. Remain alert and cautious in regard to the security of Department-owned or seized firearms, or any other weapon(s). Firearms must be under the immediate control of an employee at all times, unless locked in a vehicle, or gun locker.
11. Close any secure door found propped open.

**B. Commanders are responsible to:**

1. Ensure the security of the units within their command and establish security procedures as needed.
2. Where access is electronically controlled, regularly review and modify as needed the list of persons programmed for access to their units.
3. Restrict 24-hour electronic access to their units to assigned employees/volunteers and/or in accordance with the Authorized Access List, Appendix A, except as authorized by an approved (APD-515 or APD-515A) Police Facilities Special Access Request.
4. Request keys and/or electronic card access for employees newly assigned to their units, using (APD-515A Key/Card Request). Requests should be made in

advance of the assignment whenever possible. Requests should include the access the employee will require.

5. Immediately retrieve keys and/or access card or notify the *Facilities & Security Management Section* for reprogramming when circumstances dictate restricting a card-holder's access to Police facilities; and notify the Facilities and Security Management *Section Commander* of the action taken.
6. During normal business hours the Watch Commander shall immediately notify the *Facilities and Security Management Section* of a reported loss of any electronic security access card, or the loss of any key used within any Police facility. After normal business hours, the Watch Commander shall notify the *Facilities and Security Management Section Commander* by voice mail message or e-mail. If the Watch Commander feels that the loss would compromise security at the location accessed by the card or key, immediate contact to the Security Manager by telephone shall be made. If the Security Manager is not able to be reached by telephone, calls by succession of command for the Facilities and Security Management *Section* shall be made until proper notification is complete.
7. Complete an Access Report Request when an investigative matter occurs. (See Appendix B for form APD-0609.)

C. The *Facilities and Security Management Section* is responsible to:

1. Restrict access to the security program.
2. [REDACTED]
3. Program and issue electronic access cards.
4. Issue keys only to authorized individuals.
5. Disable electronic access cards reported as lost, or upon being notified by a Commander or *Office of Internal Affairs and Professional Responsibility*.
6. Verify separating employees return keys to Facilities and Security Management Section.
7. Screen contractors and vendors prior to issuing access cards or keys.
8. Provide the Atrium Security Post with an adequate supply of visitor passes.
9. Process approved Access Report Requests.
10. Maintain a log of Access Report Requests.

D. The **Facilities and Security Management *Section Commander*** is responsible to:

1. Oversee administration of security systems and procedures including issuing of keys, key control records and lock change authorizations.
2. Ensure that contract workers are screened and monitored as appropriate to the sensitivity and confidentiality of the Police work area.
3. Oversee the private security vendor's contract. Ensure that the vendor's performance meets the Department's expectations and requirements on the contract. Initiate any actions necessary to correct deficient performance.
  - a. A private security vendor shall continuously monitor all electronic security alarms and video surveillance. Further requirements of the private security vendor are detailed in the Police Headquarters Post Orders.

E. *Under the supervision of the Facilities and Security Management Section Commander, the private security contractor* is responsible to:

1. Screen visitors *and contractors* to selected police offices in the Police Headquarters Facility.
2. Issue visitor passes to persons that will go beyond the security checkpoint in the Atrium at Police Headquarters.
3. Monitor electronic security alarms and video surveillance *and access control system*.
4. Assist in developing security procedures and alarm responses.
5. Maintain a General Services contractor's log-in sheet and afterhours log-in book for General Service employees responding to APD emergency calls.
6. Maintain a set of keys for General Services to sign in and out in order to gain access to specific areas and the facility if responding to an afterhours emergency call.

F. The ***Human Resource and Training Division Commander*** is responsible to:

1. Notify the Facilities and Security Management *Section Commander* when an employee is hired, giving 48 hours notice if possible, providing the information necessary to issue electronic access cards.
2. Immediately notify the Facilities and Security Management *Section Commander* and the *Facilities Security Management Section Office* when an employee is transferred or separated from the Department.

**6.1.05 KEYS AND ELECTRONIC ACCESS CARDS**

- A. *The Facilities Security Management Section Office* will issue electronic access cards and keys to employees for basic access as authorized by an approved (APD-515A Key/Card Request), and for special access as authorized by an approved (APD-515) Police Facilities Special Access Request Non-Employee.
- B. When authorized by a Commander, the *Facilities and Security Management Section Office* may issue cards to City officials, employees of other City agencies and contractor employees who frequently visit Police Facilities. In the case of contractors, an ending date is required. When displayed, this identification constitutes authorization for the cardholder to enter Police Facilities or other work site without signing in at the Atrium Security Post.
- C. All key duplication is coordinated through the *Facilities and Security Management Office*. Any other duplication is prohibited.
- D. [REDACTED]
- E. Requests for lock or key changes will be made by the unit commander or higher authority to the Facilities and Security Management *Section Commander*.
- F. Keys shall not be loaned, borrowed, transferred or duplicated without proper authority and documentation by Facilities and Security Management *Section Commander*.
- G. Locks shall not be added, changed or re-keyed without approval of the Facilities and Security Management *Section Commander*.
- H. Employees should consider prior arrangements to deal with possible lockouts. In the event of a lockout, employees should first request assistance from colleagues and request callback of Facilities and Security Management staff only in urgent or emergency circumstances.
- I. Financial responsibility will be assessed for costs resulting from failure to comply with key control policies and prohibitions.

**6.1.06 EMPLOYEE AND VISITOR IDENTIFICATION**

- A. The Property and Evidence Section will issue police credentials to sworn employees, authorized civilian staff and others as approved by the Chief of Police. Police credentials are produced by the Crime Scene Investigations Section.
- B. The *Facilities and Security Management Office* will issue photo identification to graduates of the Citizens' Police Academy and, when authorized by the Chief of Police, to City officials, or employees of other City agencies.
- C. Employees are expected to become familiar with the Citizens' Police Academy identification and to offer visiting graduates the same courtesy, consideration and assistance afforded other employees, volunteers and guests.
- D. Upon retirement or separation from service, police credentials and electronic access cards must be surrendered to the Property and Evidence Section.

**6.1.07 VISITORS TO POLICE FACILITIES**

- A. **Weapons**  
No weapons, including handguns or knives, may be brought into or possessed in Police facilities without prior authorization of the Chief of Police.
- B. Persons visiting secure areas of Police facilities, who do not possess a Department-issued identification, may be required to log in at the Atrium Security Post and to obtain and display a visitor's pass.
- C. Employees expecting visitors at the Police Headquarters Facility will notify the Atrium Security Post *and the Facilities and Security Management Office* in advance with the visitor's name, affiliation, and expected arrival time.
- D. Employees are prohibited from opening secure exterior or interior doors for persons who do not have a proper identification or pass at all Police facilities. *Supervisors are responsible for ensuring that visitors sign in the visitors log book if required.*
- E. All police facilities are considered Secure Areas. Visitors will be escorted by an employee of the office or unit being visited. The Special Police Officer or Private Security Officer located at the Atrium Security Post at Police Headquarters will not be utilized for the purpose of escorting visitors.
- F. Any visitor (including contractors and vendors) seeking unescorted access to Police facilities must comply with the requirements in the FBI's Criminal Justice Information Services (CJIS) Security Policy. The Information Services Section Commander should be consulted prior to the visitor's arrival in order to facilitate compliance.

G. Employees are prohibited from giving contractors or vendors access to enter or work in electrical, mechanical or telephone rooms, except entry/work may be authorized as follows:

Location	May authorize contractor or vendor entry/work
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

H. [REDACTED]

**6.1.08 FOREIGN VISITORS**

A. The Office of the Chief of Police will maintain a log of all foreign officials (both civilian and police personnel from outside the United States) visiting the Police Department, participating in ride-alongs, and requesting interviews with Department personnel.

B. The log will contain the following information:

1. The name of the visitors;
2. The location from where they are visiting;
3. Who escorted them;
4. Total staff hours used; and
5. The reason for the visit.



- C. The log will be maintained from July 1 of the current year to June 30 of following year (i.e., 07-01-2014 through 06-30-2015).
- D. All employees taking action to honor such a request when the Office of the Chief of Police is closed will document and forward the above information to the Office of the Chief of Police.

### 6.1.09 SPECIAL VISITORS AND EVENTS

- A. The Police Headquarters Facility Fitness Center and meeting/conference rooms are intended for the use of Police and DEC employees. Visitors may use the meeting/conference facilities only when: Participating in a program or event sponsored and monitored by the Police or DEC; or when personally invited and accompanied by a Police or DEC employee. Use of the Fitness Center and equipment is limited to current Police Department, DEC employees and active Police Department Volunteers. Guests, including family members, are not permitted to use the Fitness Center or equipment.
- B. The Police Headquarters Facility Community Room may be used by community groups with the approval of the *Assistant Director* for the Administrative Services Bureau. Approval will not be given *to community groups* for commercial ventures.
- C. With the approval of the *Assistant Director* for the Administrative Services Bureau, the requirement for signing in at the Atrium Security Post and displaying visitor passes may be suspended for special events such as promotional ceremonies, volunteer recognition day, holiday party, etc.
- D. Units sponsoring after-hours special events must comply with all existing security requirements.

*Generally, Police facilities will not be used to promote commercial ventures so as to preclude the perspective the activity is designed to promote an individual business or business interest. This does not apply to:*

- 1. Vendors which are invited into the facility by the department to provide information on products which the department may be considering for use in police business or as part of the normal procurement processes for the department.*
- 2. Vendors invited by the department to provide estimates as part of the procurement process for facility maintenance, repair, or improvements.*
- 3. Vendors contracted by the department to provide services within the facility.*
- 4. This also does not apply to activities by non-profit entities that may be approved by the Chief of Police.*

**6.1.10 OTHER POLICE FACILITIES**

- A. The Range Manager, K-9 Supervisor, and the ranking commander at other Police facilities will develop security plans and procedures for their respective facilities and provide a copy to the *Facilities and Security Management Section Commander*.
- B. Employees will maintain the security of satellite facilities by keeping lock combinations confidential, securing the facility upon leaving, and immediately reporting any lock or security issues to the *Facilities and Security Management Section Commander*.

**6.1.11 EMERGENCIES**

**A. Emergency Access to Police Headquarters Offices**

For the purposes of this plan, an emergency will be deemed any reason that would lead a reasonable person to believe that a delay in entering an office at the Police Headquarters could lead to bodily harm to another, prevent the loss or damage of irreplaceable property, and/or other matters that can be properly justified by the entering party.

In the event an officer finds it necessary to access an office at Police Headquarters, they will immediately notify the Watch Commander of the location they are about to enter. This is done for officer safety and for alarm notification. The Watch Commander will notify the Security Officers at the Atrium Security Post of the officer's full name who is in route.

[REDACTED]

The commander or supervisor of the office will also be notified of the entry and respond to the office if necessary. The Watch Commander will ensure the *Assistant Chief* of the *Field Operations Bureau* is notified, and this entry is noted on the Watch Commander's Report.

This plan does not include emergency access to the *Office of Internal Affairs and Professional Responsibility* office, the Personnel and Training file room, Property & Evidence Section, the Computer Crimes Lab and the office of the Chief of Police. If emergency access is needed for one of these areas, the Watch Commander must be notified. The Watch Commander may authorize DEC to request personnel from the Facilities and Security Management Section or the affected Unit respond and gain entry, [REDACTED].

**B. Alarms**

In the absence of prior notice that testing is underway, commanders will ensure that employees immediately leave the building when the fire alarm sounds. As they leave, employees will secure confidential information and close all doors. Employees may return to the building only when advised by Fire Department staff that it is safe to do so.

**By Authority Of:**

**Michael L. Brown  
Chief of Police**

# Appendix A

## Security of Police Facilities

### Authorized Access Categories

#### A. General Headquarters Office Areas

All sworn and civilian staff will have access to electronically controlled doors during normal business hours (0800 – 1600) Monday through Friday for the following areas:

- Administration (3<sup>rd</sup> Floor Office Suite)
- Criminal Investigations Section
- Facilities and Security Management Section
- [Human Resources](#) and Training Division
- Technical Support Unit
- [Audits](#), Accreditation and Directives Section
- Tactical Computers Unit

#### B. Special Headquarters Access Areas

All sworn and civilian staff will have access to the following areas during the times listed.

- Crime Scene Investigations front entry – Monday through Friday, 0700 – 1530 hours.

#### C. Restricted Headquarters Access Areas

Only authorized sworn and civilian staff will have access to following areas.

- Information Services Section
- Tactical Anti-Crime Section
- Property & Evidence Section
- Computer, Radio & Telephone/Security Rooms
- Office of the Chief of Police
- [\*Office of External Affairs and Professional Responsibility\*](#)

#### D. Department of Emergency Communications

Access to the Department of Emergency Communications office at Police Headquarters is controlled by its Director. Request for access to DEC shall be made through a Police commander directly to the DEC Director.

**E. Public Safety Center (Mill Road)**

Access to the facility is controlled by the Office of Sheriff. Sworn staff will have access to areas within the facility as approved by the Office of Sheriff. Selected civilian staff will have access to areas within the facility. The *Facilities and Security Management Section* is the liaison with the Office of Sheriff for all access issues at the Public Safety Center.

**F. Other Facilities**

Access to all other Police facilities will be at the discretion of the commander of those facilities.